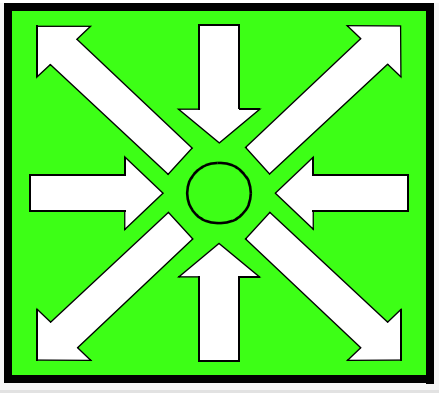
Cisco Router



Supports Management Module SM-CIS1001

APRISMA SPECTRUM® POWERED SOLUTIONS

Device Management

Copyright Notice

Document 9030809-04. Copyright © April 2002 by Aprisma Management Technologies, Inc. All rights reserved worldwide. Use, duplication, or disclosure by the United States government is subject to the restrictions set forth in DFARS 252.227-7013(c)(1)(ii) and FAR 52.227-19.

Liability Disclaimer

Aprisma Management Technologies, Inc. (“Aprisma”) reserves the right to make changes in specifications and other information contained in this document without prior notice. In all cases, the reader should contact Aprisma to inquire if any changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL APRISMA, ITS EMPLOYEES, OFFICERS, DIRECTORS, AGENTS, OR AFFILIATES BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF APRISMA HAS BEEN ADVISED OF, HAS KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Trademark, Service Mark, and Logo Information

SPECTRUM, **IMT**, and the **SPECTRUM IMT/VNM** logo are registered trademarks of Aprisma Management Technologies, Inc., or its affiliates. **APRISMA**, **APRISMA MANAGEMENT TECHNOLOGIES**, the **APRISMA MANAGEMENT TECHNOLOGIES** logo, **MANAGE WHAT MATTERS**, **DCM**, **VNM**, **SpectroGRAPH**, **SpectroSERVER**, **Inductive Modeling Technology**, **Device Communications Manager**, **SPECTRUM Security Manager**, and **Virtual Network Machine** are unregistered trademarks of Aprisma Management Technologies, Inc., or its affiliates. For a complete list of Aprisma trademarks, service marks, and trade names, go to http://www.aprisma.com/manuals/trademark-list.htm.

All referenced trademarks, service marks, and trade names identified in this document, whether registered or unregistered, are the intellectual property of their respective owners. No rights are granted by Aprisma Management Technologies, Inc., to use such marks, whether by implication, estoppel, or otherwise. If you have comments or concerns about trademark or copyright references, please send an e-mail to spectrum-docs@aprisma.com; we will do our best to help.

Restricted Rights Notice

(Applicable to licenses to the United States government only.)

This software and/or user documentation is/are provided with RESTRICTED AND LIMITED RIGHTS. Use, duplication, or disclosure by the government is subject to restrictions as set forth in FAR 52.227-14 (June 1987) Alternate III(g)(3) (June 1987), FAR 52.227-19 (June 1987), or DFARS 52.227-7013(c)(1)(ii) (June 1988), and/or in similar or successor clauses in the FAR or DFARS, or in the DOD or NASA FAR Supplement, as applicable. Contractor/manufacturer is Aprisma Management Technologies, Inc. In the event the government seeks to obtain the software pursuant to standard commercial practice, this software agreement, instead of the noted regulatory clauses, shall control the terms of the government's license.

Virus Disclaimer

Aprisma makes no representations or warranties to the effect that the licensed software is virus-free.

Aprisma has tested its software with current virus-checking technologies. However, because no antivirus system is 100 percent effective, we strongly recommend that you write-protect the licensed software and verify (with an antivirus system in which you have confidence) that the licensed software, prior to installation, is virus-free.

Contact Information

Aprisma Management Technologies, Inc.
273 Corporate Drive
Portsmouth, NH 03801

Phone:	603-334-2100
U.S. toll-free:	877-468-1448
Web site:	http://www.aprisma.com

Contents

INTRODUCTION 7

Purpose and Scope 7
Required Reading 7
Supported Devices 8
The SPECTRUM Model 9

TASKS 11

EVENTS 14

CISCOVIEW 15

DEVICE VIEW 17

Interface Device View 17
Interface Icons 18
Interface Icon Subviews Menu 20
Secondary Address Panel View 21

DEVICE TOPOLOGY VIEW 22

Interface Device Topology View 22
Sub-Interfaces Topology View 23

APPLICATION VIEW 24

Main Application View 24
Supported Applications 25
Common Applications 25
Device-Specific MIBs 26
Generic Routing Applications 28
IP Routing Application 29
Cisco IP Accounting Table View 29
Novell Routing Application 30
Novell Service Advertisement Protocol (SAP) View 30
Novell Internet Packet Exchange (IPX) View 30
Check Point Information 30
IPX Accounting Information 30
Check Point Accounting Table 31
Accounting Table 31
Vines Routing Application 32
Vines Routing Echo View 32
Vines Routing ICP View 32
Vines Broadcast Detail View 33
Vines Rx View 34
Vines Tx View 34
XNS Routing Application 35
Cisco BSTUN Application 35
BSTUN Groups View 35
BSTUN Ports View 36
BSTUN Routes View 37
Cisco STUN Application 37
STUN Group View 38
STUN Port View 38
STUN Route View 39

Contents

Cisco Chassis Application 40
Cisco Chassis Card View 40
Cisco Card Interface View 40
Cisco Chassis General Information View 41
Chassis Information 41
ROM Information 51
RAM Information 51
Cisco Modem Application 52
Modem System Information View 52
Modem Line Status Table View 53
Modem Line Configuration Table View 57
Modem Line Statistics Table View 59
Modem Line Speed Statistics Table View 60
Cisco Flash Application 61
Cisco Flash Configuration View 62
Flash Directory 62
Flash Device Chip Properties Table View 62
Flash Copy Operations Table View 63
Flash Device Properties Table View 65
Flash File Properties Table View 65
Flash Miscellaneous Operations Table View 66
Flash Device Partition Properties Table View 66
Flash Partitioning Operations Table View 67
Cisco Ping Application 68
Ping Request Entry View 68
Ping Request Entries 68
Saved Ping Requests 69
Cisco Queue Application 71
Queue Interface View 71
Queue Statistics View 71
Queue Rotation Interface View 72
ATM Client Application 72
VCL Table 72
ATM Link Modeling Options 74
Creating VPL/VCL Models 75
Destroying VPL/VCL Models 75
EnvMon Application 76
Enable Notifications 76
Fan Status 76
Power Supply Status 77
Temperature Status 77
Voltage Status 77
Discovery Application 78
Discovery Cache Table View 78
Interface Discovery Status Table 79
Cisco Interface Application 80
CiscoIfceApp Configuration 80
Cisco Terminal Server Application 80
Line Configuration View 80
Cisco Terminal Server Line View 81
Cisco Terminal Server Session View 82
Cisco Memory Pool Application 83
Cisco Memory Pool Monitor Table View 83
Cisco Syslog Application 84
Cisco Syslog Message Filter View 84
Cisco SysLog Basic Configuration View 85
Cisco SysLog History Table View 86
Cisco IPM Routing Application 87
IPM Route Table View 87
IPM Route Table 87

Contents

IPM Route Next Hop Table View 88
IPM Route Next Hop Table 88
IPM Route Interface Table View 90
IPM Route Interface Table 90
IPM Route Boundary Table View 90
IPM Route Boundary Table 90
Cisco IPM Route Table View 91
Cisco IPM Route Table 91
Cisco IPM Route Next Hop Table View 93
Cisco IPM Route Next Hop Table 93
Cisco IPM Route Heartbeat Table View 94
Cisco IPM Route Heart Beat Table 94
Cisco PIM Application 95
PIM Interface Table View 96
PIM Interface Table 96
PIM Neighbor Table View 97
PIM IPM Route Table View 97
PIM IPM Route Table 97
PIM Rendezvous Point Sets Table View 98
Rendezvous Point Sets Table 98
PIM IPM Route Next Hop Table View 99
PIM IPM Route Next Hop Table 99
PIM Candidate Rendezvous Point Table View 100
PIM Candidate Rendezvous Point Table 100
PIM Component Table View 101
PIM Component Table 101
Cisco PIM Objects View 102
Cisco VPDN Application 104
Cisco VPDN System Info View 104
Cisco VPDN Tunnel Attribute View 105
Cisco VPDN Tunnel Session View 107
Cisco VPDN User Failure History View 109
Cisco DLSW Ext Application 111
Cisco DLSW Ext Node View 111
Cisco DLSW Ext Transport Connection Config View 116
Cisco DLSW Ext Transport Connection Operation View 119
Cisco DLSW Ext Transport Connection Specific View . 121
Cisco DLSW Ext Transport Connection Direct Config View 121
Cisco DLSW Ext Interface View 122
Cisco DLSW Ext Fast View 123
Cisco DLSW Ext Circuit View 124
Cisco DLSW Ext Trap Control View 125
Cisco DLSW Application 125
Cisco DLSW Node View 126
Cisco DLSW Transport Connection Statistics View 129
Cisco DLSW Transport Connection Config View 129
Cisco DLSW Transport Connection Operation View 132
Cisco DLSW Transport Connection TCP Config View.. 137
Cisco DLSW Transport Connection TCP Operation View 138
Cisco DLSW Interface View 138
Cisco DLSW Dir MAC Cache View 139
Dlsw Dir MAC Table 139
Cisco DLSW Dir NBIOS Cache View 141
Dlsw Dir NBIOS Table 141
Cisco DLSW Dir Location View 143

Dlsw Dir Locate Mac Table 143
Dlsw Dir Locate NBIOS Table 143
Cisco DLSW Circuit View 143
Dlsw Circuit Table 144
Cisco DLSW SDLC View 148
Dlsw LS Table 148
Cisco HSRP Application 149
Cisco HSRP Group Table View 150
HSRP Group Table 150
Cisco HSRP Group Tracked Interface Table View 153
Cisco Secondary HSRP IP Address Table View . 154
Cisco HSRP Physical Interface Configuration Table View 155

PERFORMANCE VIEWS **156**

Performance View 156
Device Performance View 157
Cisco Processes CPU Statistics Table View 158

CONFIGURATION VIEWS **159**

Device Configuration View 159
Redundancy and Model Reconfiguration Options View 160
Cisco Memory Pool Monitor Table View 161
Cisco Config-Copy Table View 162
Cisco Running Config Event/Alarm Configuration View 165

SYSLOG TRAP SUPPORT **166**

MODEL INFORMATION VIEW **169**

INDEX **175**

Contents

Introduction

This section introduces the SPECTRUM Device Management documentation for Cisco Router devices.

This introduction contains the following topics:

- *Purpose and Scope*
- *Required Reading*
- *Supported Devices* (Page 8)
- *The SPECTRUM Model* (Page 9)

Purpose and Scope

Use this document as a guide for managing the Cisco Router devices described on Page 8 with SPECTRUM management module SM-CIS1001. The document describes the icons, menus, and views that enable you to remotely monitor, configure, and troubleshoot Cisco Router devices through software models in your SPECTRUM database.

Information specific to SM-CIS1001 is included in this document. For general information about device management using SPECTRUM and for explanations of basic SPECTRUM functionality and navigation techniques, refer to the topics listed under *Required Reading*.

Required Reading

To use this documentation effectively, you must be familiar with the information covered by the other SPECTRUM online documents listed below.

- ***Getting Started with SPECTRUM for Operators***
- ***Getting Started with SPECTRUM for Administrators***
- ***How To Manage Your Network with SPECTRUM***
- ***SPECTRUM Views***
- ***SPECTRUM Menus***
- ***SPECTRUM Icons***
- ***SPECTRUM Software Release Notice***

Supported Devices

SPECTRUM management module SM-CIS1001 currently lets you model the Cisco Routers listed below.

700 series: includes the 751, 752, 753, 761, 762, 765, 766, 771, 775, 776.

800 series: includes the 801, 802, 803, 804, 805.

1000 series: includes the 1000, 1003, 1004, 1005, 1020, 1401, 1503, 1601, 1603, 1604, 1605.

2000 series: includes the 2000, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2521, 2522, 2523, 2524, 2525, 2610, 2611, 2612, 2613, 2620, 2621.

3000 series: includes the 3000, 3101, 3102, 3104, 3202, 3204, 3620, 3640, 3660.

4000 series: includes the 4000, 4500, 4700.

6000 series: includes the 6200, 6400.

7000 series: includes the 7000, 7010, 7202, 7204, 7206, 7507, 7507z, 7507mx, 7505, 7576.

8000 series: includes the 8510, 8515.

Pro Series: includes the Pro1003, Pro1004, Pro1005, Pro2500PCE, Pro2501, Pro2503, Pro2505, Pro2507, Pro2509, Pro2511, Pro2514, Pro2516, Pro2519, Pro2520, Pro2521.

12000 GSR Series

Access Pro Series: includes the AccessProRC, AccessProEC.

Other devices managed: IGS, AGS, AGSplus, CGS, MGS, MIM, ciscoGatewayServer, ciscoTerminalServer, ciscoTrouter, ciscoProtocolTranslator, ciscocs500 (ciscoAS2509RJ), (ciscoAS2511RJ), cisco2501FRADFX, cisco2501LADFRADFX, cisco2502LADFRADFX, ciscoWSX5302, ciscoFastHub216T, ciscoMicroWebserver2, ciscoFastHubBMMTX, ciscoFastHubBMMFX, ciscoSC3640, ciscoRMP, cisco6400Nrp, cisco7206VXR, cisco7204VXR, cisco1538M, ciscoFasthub100, ciscoPIXfirewall, ciscoMGX8850, ciscoMGX8830, ciscoIGX8410, ciscoIGX8420, ciscoIGX8430, ciscoIGX8450, ciscoBPX8620, ciscoBPX8650, ciscoBPX8680, ciscoCacheEngine, ciscoIGXSes, ciscoMGX8240, ciscoWSX6302Msm, cisco7120QuadT1, cisco7120T3, cisco7120E3, ciscoAt3, cisco7120Ae3, cisco7120Smi3, cisco7140Dualt3.

The SPECTRUM Model

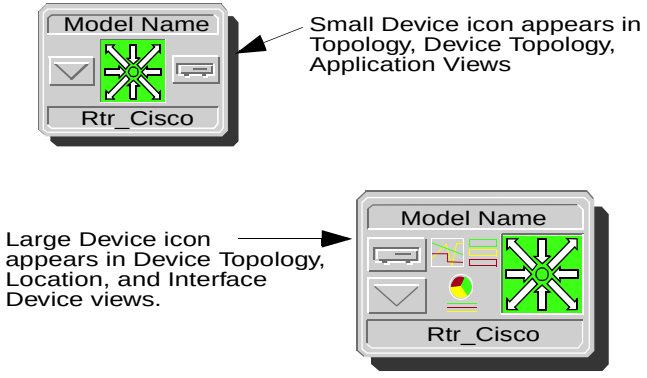
The model type for the Cisco Router devices is **Rtr_Cisco**.

Modeling results in the creation of Device icons that represent the devices and Application icons that represent their supported applications.

The Device icons contain double-click zones and provide access to Icon Subviews menus that let you perform device management activities such as those listed in *Tasks* on Page 11.

As Figure 1 shows, the Device icon varies slightly depending on the kind of view in which it appears.

Figure 1: Device Icons


Model Name
Rtr_Cisco
Small Device icon appears in Topology, Device Topology, Application Views
Large Device icon appears in Device Topology, Location, and Interface Device views.
Model Name
Rtr_Cisco

The device-specific Icon Subviews menu options available from the Device icon are listed below.

Option	Accesses the...
Performance	*Performance Views* (Page 156)
Fault Management	Fault Management view, which is described in the ***How to Manage Your Network with SPECTRUM*** documentation.
Device	*Device View* (Page 17)
DevTop	*Device Topology View* (Page 22)
Application	*Application View* (Page 24)
Device Performance	*Device Performance View* (Page 157)
Configuration	*Configuration Views* (Page 159)
Model Information	*Model Information View* (Page 169)
Primary Application	Menu options that let you select the primary application (for example, Routing, Gen Bridge App, or MIB-II).

The rest of this document covering management module SM-CIS1001 is organized as follows:

- *Tasks* (Page 11)
- *Events* (Page 14)
- *CiscoView* (Page 15)
- *Device View* (Page 17)
- *Device Topology View* (Page 22)
- *Application View* (Page 24)
- *Performance Views* (Page 156)
- *Configuration Views* (Page 159)
- *Syslog Trap Support* (Page 166)
- *Model Information View* (Page 169)

Tasks

This section lists in alphabetical order various management and troubleshooting tasks that can be performed for the Cisco Router using the views, icons, and labels referenced in this document.

Active Sessions (check)

- *Cisco VPDN System Info View* (Page 104)

Applications Supported (check)

- *Supported Applications* (Page 25)

CiscoView (launch)

- *CiscoView* (Page 15)

Connections (set)

- *Local Ack* (Page 36)
- *Cisco Terminal Server Line View* (Page 81)

Device (configure)

- *Secondary Address Panel View* (Page 21)
- *Cisco Chassis General Information View* (Page 41)
- *Modem System Information View* (Page 52)
- *Flash Directory* (Page 62)
- *Configuration Views* (Page 159)

Environment Variables (set)

- *EnvMon Application* (Page 76)

Heart Beat Interval (check/change)

- *Cisco IPM Route Heart Beat Table* (Page 94)

IPM Packets Received (check)

- *IPM Route Table* (Page 87)

IPM Packets Forwarded (check)

- *IPM Route Next Hop Table* (Page 88)

IPM Route (enable)

- *IPM Route Table* (Page 87)

IPM Routing Protocol (check)

- *IPM Route Table* (Page 87)
- *IPM Route Next Hop Table* (Page 88)
- *IPM Route Interface Table* (Page 90)
- *Cisco IPM Route Table* (Page 91)

Join/Prune Interval (check/change)

- *PIM Interface Table* (Page 96)

LANs (create)

- *Discover LANs* (Page 161)

Messages (create)

- *Events* (Page 14)

Multicast Packets In/Out (check)

- *IPM Route Interface Table* (Page 90)

Outgoing Interface/Next Hop State (check)

- *IPM Route Next Hop Table* (Page 88)

Performance (check)

- *Interface Device View* (Page 17)
- *Device Performance View* (Page 157)

Ping Request List (update)

- *Ping Request Entry View* (Page 68)

Port (configure)

- *IP Address Label* (Page 19)
- *Configuration Views* (Page 159)

Port Route Settings (check)

- *STUN Port View* (Page 38)

Redundant Addresses (enable/disable)

- *Redundancy and Model Reconfiguration Options View* (Page 160)

Status (check/change)

- *IPM Route Boundary Table* (Page 90)
- *Cisco IPM Route Heart Beat Table* (Page 94)
- *PIM Interface Table* (Page 96)
- *PIM Candidate Rendezvous Point Table* (Page 100)

Thresholds (set)

- *IPX Accounting Information* (Page 30)
- *Model Information View* (Page 169)

Upstream Neighbor Address (check)

- *IPM Route Table* (Page 87)

View IF/Port/App Statistics

- *Interface Device View* (Page 17)
- *Interface Icons* (Page 18)

View/Change Interface IP Address

- *Secondary Address Panel View* (Page 21)

View Current Interface/Port Status

- *Interface Device View* (Page 17)
- *Configuration Views* (Page 159)

Events

This section provides the range of event messages that are specific to the Cisco Router.

The Cisco Router has several event and alarm messages that are specific to its devices. If these messages are not sufficient and you wish to create your own messages, or view the existing messages for the Router, you can do so using the ***ECEditor***.

The event messages for the Router, which range from **Event03250000 to Event03250002**, can be found in the following directory:

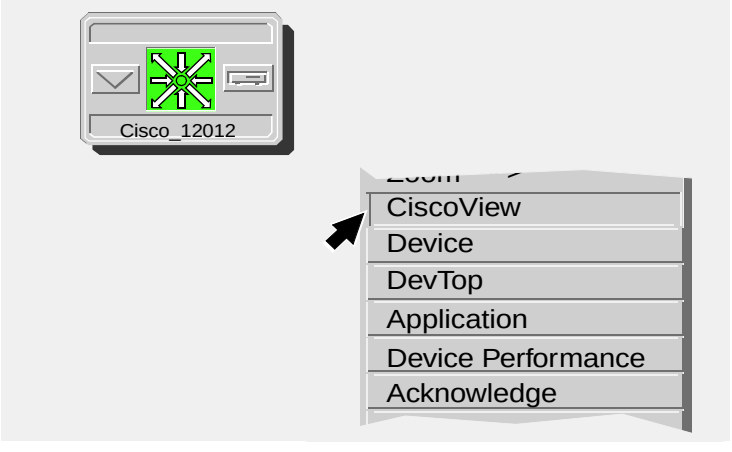
<install area>/SG-Support/CsEvFormat

CiscoView

This section describes how to access Cisco's CiscoView management software from SPECTRUM.

CiscoView is management software specific to Cisco Routers.

The Cisco_Rtr model type provides a menu option from the Device icon that is used to launch CiscoView.



For Solaris
Add the following information to the `/opt/SPECTRUM/spectrum60.env` file:

```
#CiscoView 3.0

CVIEW =<path_to_ciscoview>
```

For Windows NT and Windows 2000
From the Start > Run window, type

`regedit` (registry editor)

Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Aprisma Management Technologies > Spectrum60 > Environment**

Choose **Edit > New > String Value**

Type `CVIEW` for the name, and `<path_to_ciscoview>` as the string value.

Note:

CiscoView 3.0 will appear as "Cisco View" on your device menu after the above steps have been followed. This should not be confused with "CiscoView", which denotes the CiscoWorks 2000 CiscoView. The CiscoWorks 2000 menu picks will only appear in the device menu if the SPECTRUM Adapter script has been run. See the CiscoWorks 2000 documentation for further information.

Device View

This section describes the Device view and its associated subviews for models of Cisco Router devices in SPECTRUM.

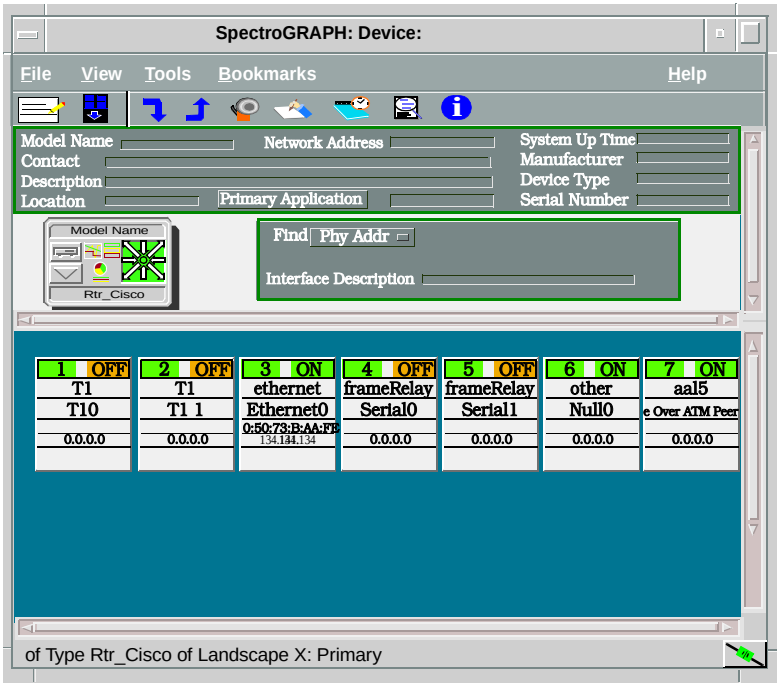
Device views use icons and labels to represent the modeled device and its components, such as modules, ports, and applications. There is one type of Device view for Rtr_Cisco models, the Interface Device View.

Interface Device View

Access: *From the* ***Icon Subviews*** *menu for the Interface icon, select* ***Device****.*

This view provides dynamic configuration and performance information for each of the device's serial/network I/O ports, which are represented by Interface icons in the bottom panel of the view, as shown in Figure 2. The middle panel of the view also displays a Device icon, which allows you to monitor the device operation and access other device-specific views.

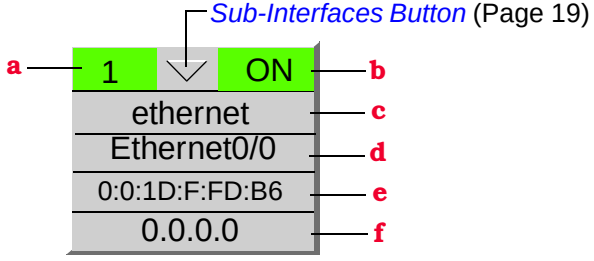
Figure 2: Interface Device View



Interface Icons

Figure 3 illustrates an Interface icon from the Interface Device view. Most of the informational labels on the icon also provide double-click access to other views, as explained in the following label descriptions. The **Sub-Interfaces** button only appears on certain Interface icons (see *Sub-Interfaces Button* (Page 19).

Figure 3: Interface Icon



a *Interface Number Label*

b *IF Status Label*

c *Interface Type Label*

d *Network Type Label*

e *Physical Address Label*

f *IP Address Label*

Interface Number Label

This label displays the interface (port) number.

IF Status Label

This label displays the current status of the interface for the primary application selected, e.g., Routing, MIB-II, etc. Table 1 lists the possible label color representations. Note that the color of the label also depends on the interface's current Administrative Status, which is set by the user in the Interface Configuration view. This view can be accessed by double-clicking the *Interface Type Label*.

Table 1: Interface Status Label Colors

Color	Operational Status	Administrative Status	Label Text
Green	Up	On	ON
Blue	Down	Off	OFF
Yellow	Down	On	OFF
Red	Testing	Test	Test

Interface Type Label

This label identifies the interface type (Ethernet, ATM, etc.). Double-click this label to access the Interface Configuration view. See the ***SPECTRUM Views*** documentation.

Network Type Label
This label identifies the type of network the interface is connected to. Double-click the label to open the Model Information view for the interface.

Physical Address Label
This label displays the physical (MAC) address of the interface. Double-click the label to open the Interface Address Translation table, which cross-references network addresses to MAC addresses for selected nodes between networks. Double-click any column entry to open an address-specific Address Translation Table Information view. This view provides the same information as the corresponding row for the Interface Address Translation table, but lets you modify field values.

IP Address Label
This label displays the IP address for the interface. Double-click this label to open the *Secondary Address Panel View* (Page 21), which lets you change the address and mask for the interface.

Sub-Interfaces Button
This button appears on an Interface icon when the interface model has sub-interfaces associated with it. Examples include a physical ATM interface with Permanent Virtual Circuits (PVCs) provisioned on it or a physical Frame Relay interface with DCL circuits on it. The endpoints of these multiplexed connections are modeled by SPECTRUM as sub-interfaces. Double-click this button to access the *Sub-Interfaces Topology View* (Page 23).

Interface Icon Subviews Menu

Table 2 lists the Icon Subviews menu options available for the Interface icon.

Table 2: Interface Menu Options

Option	Opens the...
Detail	Interface Detail view, which displays Packet, Error, and Discard Breakdown pie charts.
Sub-Interfaces	*Sub-Interfaces Topology View* (Page 23)
IF Configuration	Interface Configuration view (see ***SPECTRUM Views***).
Address Translation Table	Address Translation Table (AT) (see ***SPECTRUM Views***).
Secondary Address Panel	*Secondary Address Panel View* (Page 21).
Thresholds	Interface Threshold view, which lets you set the on/off alarm thresholds for load, packet rate, error rate, and % discarded for the interface.
Model Information	*Model Information View* (Page 169).

Table 2: Interface Menu Options (Continued)

Option	Opens the...
Trap Configuration	Interface Trap Configuration view (see ***How to Manage Your Network with SPECTRUM***).
Cisco Network Info	Cisco Interface Network View which displays In Packets, Out Packets, In Octets, and Out Octets pie charts.
Cisco Router Info	Cisco Interface Router View which displays generic routing applications information.
Cisco Traffic Info	Cisco Interface Traffic View which displays slow and fast traffic pie charts.
Cisco Other Info	Other Cisco Interface View which displays In Packets, Out Packets, In Octets, and Out Octets pie charts.

Secondary Address Panel View

Access: *From the **Icon Subviews** menu for the Interface icon in the Interface Device view, select **Secondary Address Panel**.*

This panel provides a table of IP addresses and masks obtained from the Address Translation table within the device's firmware. You can change the current address displayed in the **IP Address** field by selecting an entry from the table in this panel and clicking the **Update** button.

Device Topology View

This section describes the Device Topology views available for models of Cisco Router devices in SPECTRUM.

Device Topology views show the connections between a modeled device and other network entities. There are two types of Device Topology views available for models of Cisco Routers:

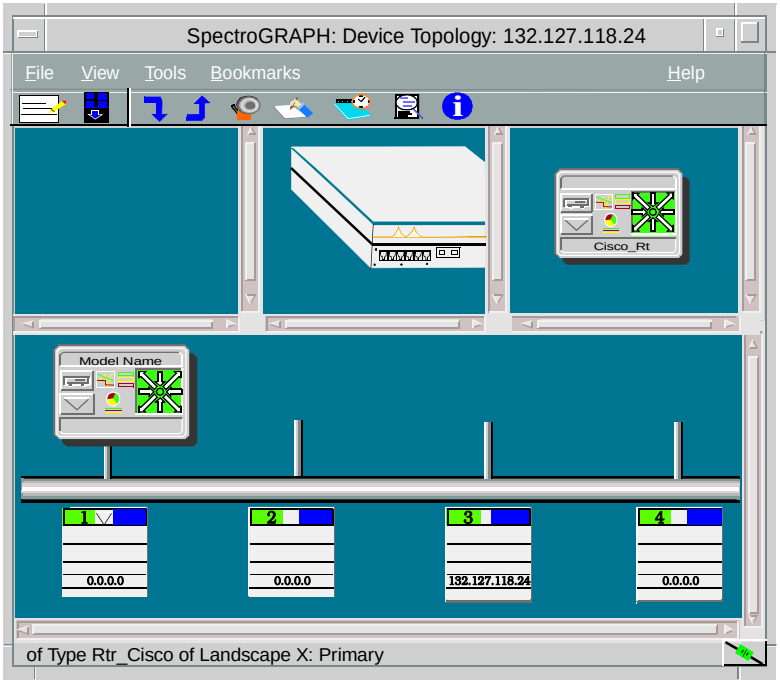
- *Interface Device Topology View*
- *Sub-Interfaces Topology View* (Page 23)

Interface Device Topology View

Access: *From the **Icon Subviews** menu for the Device icon, select **DevTop**.*

The lower panel (Figure 4) uses Interface icons to represent the device's serial/network/I/O ports. These icons provide the same information and menu options as those in the *Device View* (Page 17). If a device is connected to an interface, a Device icon appears on the vertical bar above the Interface icon along with an icon representing the network group that contains the device. See ***SPECTRUM Views*** for more details.

Figure 4: DevTop View



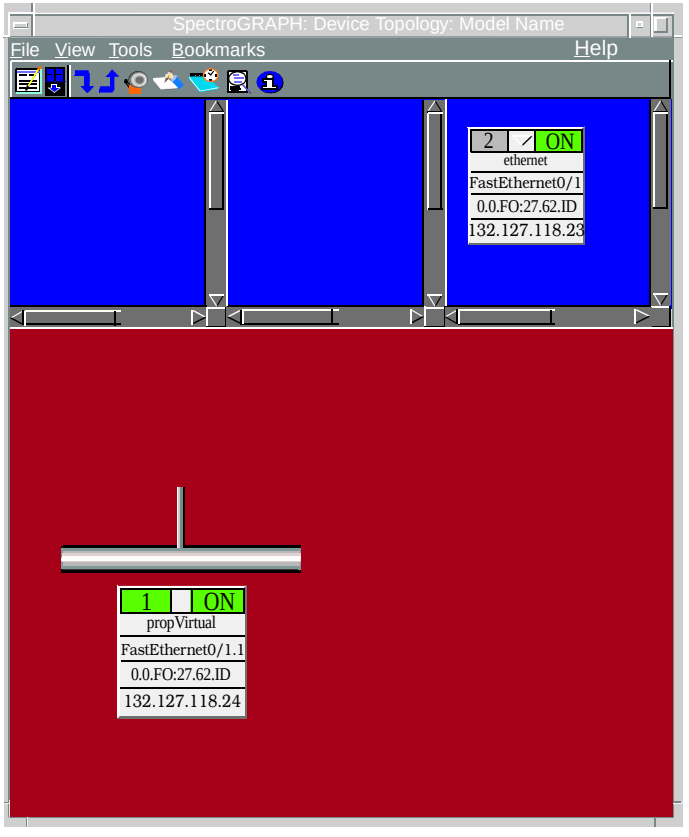
Sub-Interfaces Topology View

Access: *From the **Icon Subviews** menu for an Interface icon whose interface contains sub-interfaces, select **Sub-Interfaces**.*

When present, the endpoints associated with multiplexed, physical connections are modeled by SPECTRUM as sub-interfaces. This includes, for example, Permanent Virtual Circuits (PVCs) on a physical ATM interface and DCL circuits on a physical Frame Relay interface.

The lower panel of the Sub-Interfaces Topology view (Figure 5) uses Interface icons to represent these non-physical entities and circuits that are connected to the physical interface. These Interface icons provide the same labels and menu options as the Interface icons in the *Device View* (Page 17).

Figure 5: Sub-Interfaces Topology View



Application View

This section describes the Application view and the associated application-specific subviews available for models of Cisco Router devices in SPECTRUM.

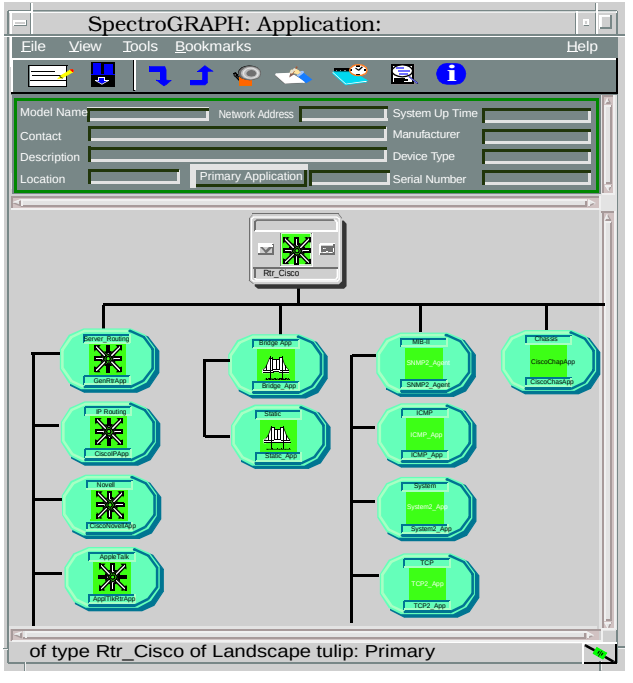
Access: *From the* ***Icon Subviews*** *menu for the Device icon, select* ***Application****.*

Main Application View

When a device model is created, SPECTRUM automatically creates models for each of the major and minor applications supported by the device. The main Application view identifies all of these application models, shows their current condition status, and provides access to application-specific subviews. Figure 6 shows this view in the Icon mode. If you prefer the List mode, which displays applications as text labels, select **View > Mode > List**.

For more information on this view, refer to the ***MIBs and the Application View*** document.

Figure 6: Main Application View



Supported Applications

SPECTRUM's applications can be grouped within two general categories as follows:

- Applications associated with non proprietary MIBs. See *Common Applications* below.
- Applications associated with device-specific MIBs. See *Device-Specific MIBs* (Page 26).

Common Applications

For the most part, these applications represent the non proprietary MIBs supported by devices. Listed below (beneath the title of the SPECTRUM document that describes them) are some of the common applications currently supported by SPECTRUM. Refer to these documents when your devices support these applications.

Note: The documents listed below (in bold font) are available for viewing at: www.aprisma.com/manuals/

- ***Routing Applications***
  - Generic Routing
  - Repeater
  - AppleTalk
  - DECnet
  - OSPF
  - OSPF2
  - BGP4
  - VRRP
  - RFC 2932
- ***Bridging Applications***
  - Ethernet Special Database
  - Spanning Tree
  - Static
  - Transparent
  - PPP Bridging
  - Source Routing
  - Translation
  - QBridge
- ***MIB II Applications***
  - SNMP
  - IP
  - ICMP
  - TCP
  - System2
  - UDP
- ***Transmission Applications***
  - FDDI
  - Point to Point
  - DS1
  - DS3

- RS-232
- WAN
- Frame Relay
- Token Ring
- Ethernet
- Fast Ethernet
- RFC 1317App
- RFC 1285App
- RFC 1315App
- 802.11App
- SONET

- ***Technology Applications***
  - APPN
  - ATM Client
  - DHCP
  - DLSw
  - PNNI
  - RFC 1316App
  - RFC 1514
  - RFC 2287
  - RFC 2790
  - RFC 2925

- ***DOCSIS Applications***
  - DOCSISCblDvApp
  - DOCSISQOSApp
  - DOCSISBPI2App
  - DOCSISBPIApp
  - DOCSISIFApp

- ***Digital Subscriber Line (DSL) Applications***
  - ADSL

Device-Specific MIBs

SPECTRUM imports the following device-level proprietary MIBs into its database:

- CISCO-BSC-MIB
- CISCO-BSTUN-MIB
- CISCO-CIPCSNA-MIB
- CISCO-CHANNEL-MIB
- CISCO-PING-MIB
- CISCO-ENVMON-MIB
- CISCO-INTERFACES-MIB
- CISCO-IP-MIB
- CISCO-NOVELL-MIB
- CISCO-TS-MIB
- CISCO-VINES-MIB
- CISCO-XNS-MIB
- CISCO-CHASSIS-MIB

- CISCO-ENV-MIB
- CISCO-DSPU-MIB
- CISCO-DLSW-MIB
- CISCO-ISDN-MIB
- CISCO-QUEUE-MIB
- CISCO-REPEATER-MIB
- CISCO-RSRB-MIB
- CISCO-SDLLC-MIB
- CISCO-SNAPSHOT-MIB
- CISCO-STUN-MIB
- CISCO-DECNET-MIB
- CISCO-CALL_HISTORY_MIB
- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- CISCO-HSRP-MIB
- CISCO-HSRP-EXT-MIB

These MIBs can be used in conjunction with SPECTRUM's optional customization products (referred to as the Level I Tool Kits) to create application models and views that display the condition of selected MIB objects.

Note: Aprisma Management Technologies can provide training, technical assistance, and custom engineering support services for creating application models and their associated views.

The following device-specific applications are described in the remainder of this section:

- *IP Routing Application* (Page 29)
- *Novell Routing Application* (Page 30)
- *Vines Routing Application* (Page 32)
- *XNS Routing Application* (Page 35)
- *Cisco BSTUN Application* (Page 35)
- *Cisco STUN Application* (Page 37)
- *Cisco Chassis Application* (Page 40)
- *Cisco Modem Application* (Page 52)
- *Cisco Flash Application* (Page 61)
- *Cisco Ping Application* (Page 68)
- *Cisco Queue Application* (Page 71)
- *ATM Client Application* (Page 72)
- *EnvMon Application* (Page 76)
- *Discovery Application* (Page 78)
- *Cisco Terminal Server Application* (Page 80)
- *Cisco Memory Pool Application* (Page 83)
- *Cisco Syslog Application* (Page 84)
- *Cisco IPM Routing Application* (Page 87)
- *Cisco PIM Application* (Page 95)
- *Cisco VPDN Application* (Page 104)
- *Cisco DLSW Ext Application* (Page 111)
- *Cisco DLSW Application* (Page 125)
- *Cisco HSRP Application* (Page 149)

Generic Routing Applications

The following applications and views are available under **GenRtrApp**:

- *IP Routing Application* (Page 29)
- *Novell Routing Application* (Page 30)
- *Vines Routing Application* (Page 32)
- *XNS Routing Application* (Page 35)
- *Cisco BSTUN Application* (Page 35)
- *Cisco STUN Application* (Page 37)

IP Routing Application

This application, with exception of the IP Accounting Table view described below, is described in detail in the ***Routing Applications*** documentation.

Cisco IP Accounting Table View

Access: *From the **Icon Subviews** menu for the CiscoIPApp Application icon, select **Accounting**.*

This view provides information about the network traffic flow between devices and includes a list of IP addresses. The IP Accounting Table view provides the following information.

Source

The source IP address for data transmitted to the destination IP address.

Destination

The destination IP address for data transmitted from the source IP address.

Packets

The total number of IP packets transmitted from the source IP address to the destination IP address.

Bytes

The total number of bytes transmitted from the source IP address to the destination IP address.

Checkpoint Accounting

This button allows you to access the Cisco Checkpoint Accounting Table. Table 3 provides definitions for the fields presented in the Accounting Table.

Table 3: Checkpoint View Information

Field	Definition
Source	The source IP address for data transmitted to the destination IP address in the checkpoint matrix.
Destination	The destination IP address for data transmitted from the source IP address in the checkpoint matrix.
Packets	The number of IP packets transmitted from the source IP address to the destination IP address in the checkpoint matrix.
Bytes	The total number of bytes transmitted from the source IP address to the destination IP address in the checkpoint matrix.

Novell Routing Application

This application (CiscoNovellApp) has three menu options. The **Detail** selection provides access to pie charts that display standard Packet Breakdown, Error Breakdown, and Discard Breakdown information. The **SAP/IPX** selection opens a submenu that accesses the following views:

- *Novell Service Advertisement Protocol (SAP) View*
- *Novell Internet Packet Exchange (IPX) View*

Novell Service Advertisement Protocol (SAP) View

Access: *From the **Icon Subviews** menu for the CiscoNovellApp Application icon, select **SAP/IPX > SAP Chart**.*

The view displays a color-coded pie chart of the following Novell SAP statistics:

- SAP Request Packets Transmitted
- SAP Reply Packets Transmitted
- SAP Request Packets Received
- SAP Reply Packets Received

Novell Internet Packet Exchange (IPX) View

Access: *From the **Icon Subviews** menu for the CiscoNovellApp Application icon, select **SAP/IPX > IPX Chart**.*

This view includes the Check Point Accounting table, Accounting table, and additional Check Point Accounting and IPX Accounting information described below.

Check Point Information

This section of the Novell (IPX) view provides the following information.

Check Point

The check point for the IPX accounting database. This MIB variable must be read and then set with the same value for the check point to succeed. The value read and then set will be incremented after a successful set request.

Check Point Age

The age of the data in the IPX checkpoint matrix.

IPX Accounting Information

This section of the Novell (IPX) view provides the following information:

Threshold
The threshold of IPX accounting records in use before IPX traffic will be unaccounted.

Age
The age of the data in the IPX data matrix.

Lost Bytes
The total bytes of lost IPX packets.

Lost Packets
The lost IPX packets due to memory limitations.

Check Point Accounting Table

The list of IPX check point accounting entries. The fields for this table are described below.

Source Address
The IPX Source address for host traffic matrix.

Destination Address
The IPX Destination address for host traffic matrix.

Number Packets
The number of IPX packets sent from source to destination.

Number Bytes
The total number of bytes in IPX packets from source to destination.

Accounting Table

This table displays the list of IPX accounting entries. The fields in the Accounting Table are described below.

Source Address
The IPX Source address for host in the checkpoint traffic matrix.

Destination Address
The IPX Destination address for host in the checkpoint traffic matrix.

Number Packets
The number of IPX packets sent from source to destination in the checkpoint matrix.

Number Bytes
The total number of bytes in IPX packets from source to destination in the checkpoint matrix.

Vines Routing Application

This application (CiscoVinesApp) has six menu options. The **Detail** selection provides access to pie charts that display standard Packet Breakdown, Error Breakdown, and Discard Breakdown information. The **Vines Specifics** selection opens a submenu that accesses the following views:

- *Vines Routing Echo View*
- *Vines Routing ICP View*
- *Vines Broadcast Detail View* (Page 33)
- *Vines Rx View* (Page 34)
- *Vines Tx View* (Page 34)

Vines Routing Echo View

Access: *From the **Icon Subviews** menu for the CiscoVinesApp Application icon, select **Vines Specifics > Echos**.*

This view displays a color-coded pie chart displaying a breakdown of Vines Echo statistics. Table 4 provides definitions for the statistics presented by the pie chart.

Table 4: Vines Echo Statistics

Statistic	Definition
MAC In	The total number of Vines MAC level Echo packets received.
MAC Out	MAC level Echo packets transmitted.
Echo In	The total number of Vines Echo packets received.
Echo Out	The total number of Vines Echo packets transmitted.

Vines Routing ICP View

Access: *From the **Icon Subviews** menu for the CiscoVinesApp Application icon, select **Vines Specifics > ICP**.*

This view displays a color-coded pie chart of Vines Interprocess Communications Protocol (ICP) statistics. Table 5 provides definitions for the statistics presented by the pie chart.

Table 5: Vines ICP Statistics

Statistic	Definition
ICP In	The total number of Vines ICP packets received.
ICP Out	The total number of Vines ICP packets transmitted.
Metric Out	The total number of Vines ICP Metric Notification packets transmitted.

Vines Broadcast Detail View

Access: *From the **Icon Subviews** menu for the CiscoVinesApp Application icon, select **Vines Specifics > Broadcasts**.*

This view displays a color-coded pie chart of Vines Broadcast statistics. Table 6 provides definitions for the statistics presented by the pie chart.

Table 6: Vines Broadcast Statistics

Statistic	Definition
Forward	The total number of Vines broadcast packets forwarded.
Received	The total number of Vines broadcast packets received.
Transmitted	The total number of Vines broadcast packets transmitted.
Not LAN	The total number of Vines broadcast packets not forwarded to all interfaces because the LAN ONLY bit was set.
Not Forward	The total number of Vines broadcast packets not forwarded to all interfaces because the OVER 4800 BPS bit was set.
No Charge	The total number of Vines broadcast packets not forwarded to all interfaces because the NO CHARGES bit was set.

Vines Rx View

Access: *From the **Icon Subviews** menu for the CiscoVinesApp Application icon, select **Vines Specifics > Rx Table**.*

This view provides the following information.

Forwarded
The total number of incoming Vines packets forwarded to another interface.

Format Error
The total number of incoming Vines packets containing header errors.

Local Destination
The total number of incoming Vines packets destined for this router.

Encapsulation Type
The Vines protocol default encapsulation type.

Echo Count
The total number of incoming IPC Echo messages.

Vines Tx View

Access: *From the **Icon Subviews** menu for the CiscoVinesApp Application icon, select **Vines Specifics > Tx Table**.*

This view provides the following information.

Forwarded
The total number of outgoing Vines packets forwarded to another interface.

Proxy Count
The total number of Proxy packets sent by this interface.

Unicasts
The total number of unicast packets generated by this interface.

IPC Count
The total number of IPC output messages sent by this interface.

IPC Error Count
The total number of IPC Error messages sent by this interface.

Broadcasts
The total number of broadcast packets generated by this interface.

B-casts Forwarded
The number of broadcast packets forwarded from another interface.

XNS Routing Application

This application (CiscoXNSApp) has two menu options that provide access to pie charts that display XNS statistics. Table 7 provides definitions for the statistics presented by the pie charts available for the **Echos** selection. The **Detail** selection provides access to pie charts that display standard Packet Breakdown, Error Breakdown, and Discard Breakdown information.

Table 7: XNS Echo Statistics

Statistic	Definition
Replies Rec	The total number of XNS Echo reply packets received.
Replies Sent	The total number of XNS Echo reply packets transmitted.
Request Rec	The total number of XNS Echo request packets received.
Request Out	The total number of XNS Echo request packets transmitted.

Cisco BSTUN Application

This application (CiscoBSTUNApp) has three menu options that provide access to the following views:

- *BSTUN Groups View*
- *BSTUN Ports View* (Page 36)
- *BSTUN Routes View* (Page 37)

These views provide configuration and operational information on the blocked tunneling implementation.

BSTUN Groups View

Access: *From the **Icon Subviews** menu for the CiscoBSTUNApp Application icon, select **BSTUN Groups**.*

This view identifies the group number and protocol type that Cisco A and Cisco B use to route BSC (Binary Synchronous Communication) traffic over the IP network. The group number must be the same in Cisco A and Cisco B to route traffic from one router to the other.

The following information is available from this view.

Index
The configured BSTUN (Block Serial Tunneling) group number. The significance of this number is that it must match the BSTUN Group number

configured in the router at the other end of the BSTUN tunnel.

Type
The protocol type for this BSTUN group.

Local Ack
Indicates whether the BSTUN connection is locally acknowledged (True) or not locally acknowledged (False).

Unroutable Transmit
The number of unroutable frames received by this group from the remote partner. They were unroutable because the address was not recognized; that is, there is no BSTUN route command configured for this address. This indicates that the configuration in this router is incompatible with the peer router.

Unroutable Receive
Count of frames received from a serial interface with an unsupported poll address. Note that there may be several ports configured within this BSTUN group; a non-zero value in this field indicates that at least one of these ports is receiving frames for which there are no BSTUN route commands configured. This indicates that the configuration in this router is incompatible with the configuration in at least one of the attached devices.

BSTUN Ports View

Access: *From the **Icon Subviews** menu for the CiscoBSTUNApp Application icon, select **BSTUN Ports**.*

This view identifies the serial interface to the BSC line for which the router is providing serial tunneling. It also identifies the BSTUN group that the interface is in and the default routing for unrecognized BSC addresses.

The following information is available from this view.

Group
The group number to which the BSTUN port belongs. Frames will only be routed to other ports (on this or another router) in the same BSTUN group.

Default Peer Type
The type of identification of the remote default partner.

Default Peer IP
The IP address of the remote default BSTUN partner, for unrecognized addresses.

BSTUN Routes View

Access: *From the **Icon Subviews** menu for the CiscoBSTUNApp Application icon, select **BSTUN Routes**.*

This view displays an entry for each address device for routing within the BSTUN group and an entry for default routing if the "bstun route all" command is configured. The following information is available for this view.

Group
The index of the BSTUN Group owning this station.

Address
The poll address of the station. A value of "256" indicates the presence of the ALL parameter on the STUN ROUTE command, which is the route for all unrecognized addresses.

Type
The type of identification of the remote partner.

IP
The IP address of the remote BSTUN partner.

Priority
The priority with which this station's traffic will be routed across the network.

Peer State
The state of the peer connection through the BSTUN tunnel.

Rx Packets
Count of frames received from the serial interface with this station's address.

Tx Packets
Count of frames transmitted at the serial interface with this station's address.

Rx Bytes
Count of bytes received from the serial interface with this station's address.

Tx Bytes
Count of bytes transmitted at the serial interface with this station's address.

Cisco STUN Application

This application (CiscoSTUNApp) has three menu options that provide access to the following views. These views provide configuration and operational information on the blocked tunneling implementation.

- *STUN Group View* (Page 38)
- *STUN Port View* (Page 38)
- *STUN Route View* (Page 39)

STUN Group View

Access: *From the **Icon Subviews** menu for the CiscoSTUNApp Application icon, select **STUN Group Table**.*

This view identifies the STUN (Serial Tunneling) group number and protocol type that Cisco A and Cisco B use to route SDLC traffic over the IP network. The table contains an entry for each STUN group defined on the router.

Group Index
The configured STUN group number.

Protocol Type
The protocol type for this STUN group.

STUN IP Address
The configured IP address used for all serial tunnelling in this router.

STUN Port View

Access: *From the **Icon Subviews** menu for the CiscoSTUNApp Application icon, select **STUN Port Table**.*

This view identifies the serial interface to the SDLC line for which the router is providing serial tunneling. It also identifies the STUN group that the interface is in and the default routing for unrecognized SDLC addresses.

Group Index
The group number to which the STUN port belongs. Frames will only be routed to other ports (on this or another router) in the same STUN group.

Default Peer Type
The type of identification of the default partner for unrecognized addresses.

Default Peer IP
The IP address of the remote default STUN partner, for unrecognized addresses.

Default Peer Serial IF
If the STUN Route Type is “serial” then this is the serial interface index of the point-to-point link to the remote partner; if STUN Route Type is “serialDirect” then the partner is in the local STUN; if STUN Route Type is “ip” then this field is “0.”

STUN Route View

Access: *From the **Icon Subviews** menu for the CiscoSTUNApp Application icon, select **STUN Route Table**.*

This view displays a table with information about specific Synchronous Data Link Control (SDLC) addresses. There is one table entry for each SDLC address configured by the STUN ROUTE command.

Station Addr
The poll address of the station. The variable "256" indicates the ALL parameter on the STUN Route command, which is the route for all unrecognized addresses.

Type
The type of identification of the remote partner.

Remote IP
The IP address of the remote STUN partner.

Serial IF
The local interface index to the remote partner.

Priority
The priority with which this station's traffic will be routed across the network.

Peer State
The state of the peer connection through the STUN tunnel.

Local Ack
Indicates if the STUN connection is locally acknowledged.

Rx Packets
Count of frames received from the serial interface with this station's address.

Tx Packets
Count of frames transmitted at the serial interface with this station's address.

Rx Bytes
Count of bytes received from the serial interface with this station's address.

Tx Bytes
Count of bytes transmitted at the serial interface with this station's address.

Cisco Chassis Application

This application (CiscoChasApp) has two menu options that provide access to the following views.

- *Cisco Chassis Card View*
- *Cisco Card Interface View*
- *Cisco Chassis General Information View* (Page 41)

Cisco Chassis Card View

Access: *From the **Icon Subviews** menu for the CiscoChasApp Application icon, select **Card Information**.*

This view provides information on the cards contained in the chassis.

Slot
The slot number in which this card is installed. If the slot number is not applicable or not determinable, this field will display "-1."

Type
The functional type of the card installed in this slot.

Description
A textual description of this card.

Software Ver.
The version number of the firmware installed on this card. If no version number is available, this field will remain empty.

Hardware Ver.
The hardware revision level of this card. If no revision level is available, this field will remain empty.

Serial No.
The serial number of this card. If no serial number is available, this field will contain a zero.

Cisco Card Interface View

Access: *From the **Icon Subviews** menu for the CiscoChasApp Application icon, select **Interface Information**.*

This table provides Chassis Interface information.

Index
The unique index identifier for the table entry.

Slot Number
Chassis slot number, or -1 if neither applicable nor determinable.

Port Number
Chassis port number, unique per port on a given card if available. If the Port Number is not

applicable to the card, then the object instance won't be populated.

Card Index
The card Index of the card in the Chassis card Table which contains this interface, or -1 if not applicable.

Enabled Connector Type
The Interface connector type currently enabled. Possible types are `not-specified`, `none`, `rj-45`, `db-40`, `db-15`, `auto-select`, `gbic-sx`, `gbic-lx`, `gbic-lh`, `gbic-cx`, `gbic-zx`, `missing`, `mmf-st`, `mmf-sc`, `rj-11`, `rj-48s`, `rj-48c`, `db-60`.

Cisco Chassis General Information View

Access: *From the **Icon Subviews** menu for the CiscoChasApp Application icon, select **General**.*

This view displays information on the chassis in which the router is installed. This view is divided into the three sections described below.

Chassis Information

This section of the Chassis General Information view provides the following physical information about the chassis.

Hardware Revision Level
The version number of the chassis hardware. If the version number is not available, this field will remain empty.

Chassis Type
The type of chassis. Possible chassis types appear in Table 8, below.

Table 8: Chassis Type

Type	Description
unknown	-
multibus	-
agsplus	-
igs	-
c2000	-
c3000	-
c4000	-
c7000	-
cs500	-
c7010	-
c2500	-
c4500	-
c2102	-

Table 8: Chassis Type (Continued)

Type	Description
c2202	-
c2501	-
c2502	-
c2503	-
c2504	-
c2505	-
c2506	-
c2507	-
c2508	-
c2509	-
c2510	-
c2511	-
c2512	-
c2513	-
c2514	-
c2515	-
c3101	-
c3102	-
c3103	-

Table 8: Chassis Type (Continued)

Type	Description
c3104	-
c3202	-
c3204	-
accessProRC	-
accessProEC	-
c1000	-
c1003	-
c1004	-
c2516	-
c7507	-
c7513	-
c7506	-
c7505	-
c1005	-
c4700	-
c2517	-
c2518	-
c2519	-
c2520	-

Table 8: Chassis Type (Continued)

Type	Description
c2521	-
c2522	-
c2523	-
c2524	-
c2525	-
c4700S	-
c7206	-
c3640	-
as5200	-
c1601	-
c1602	-
c1603	-
c1604	-
c7204	-
c3620	-
wsx3011	-
mc3810	-
c1503	-
as5300	-

Table 8: Chassis Type (Continued)

Type	Description
as2509RJ	-
as2511RJ	-
c2501FRADFX	-
c2501LANFRADFX	-
c2502LANFRADFX	-
wsx5302	-
c1605	-
c12012	-
c12004	-
c12008	-
ubr7246	Universal Broadband Router
c2610	c2600 with 1 integrated ethernet interface
c2612	c2600 with an integrated ethernet and token ring interface
c2611	c2600 with 2 integrated ethernet interfaces
ubr904	Cisco Cable Modem (ubr - universal broadband router)
c6200	Digital Subscriber Line Access Multiplexer (DSLAM)

Table 8: Chassis Type (Continued)

Type	Description
c3660	Six slot MARS Router
c7202	Modular two slot router in the cisco7200 family
c2620	c2600 platform with an onboard fast ethernet
c2621	c2600 platform with two onboard fast ethernets
rpm	Router Processor Module
c1710	VPN (Virtual Private Network) Security Router with 1 FastEthernet and 1 Ethernet interface onboard
c1720	-
c7576	Dual Independent RSP platform, 13 slots
c1401	Router with 1 ethernet and 1 ATM25 interface
c2613	c2600 with 1 integrated token ring interface
ubr7223	Universal Broadband Router
c6400Nrp	c6400 Network Routing Processor
c801	Cisco 800 platform with 1 ethernet and 1 BRI/ST

Table 8: Chassis Type (Continued)

Type	Description
c802	Cisco 800 platform with 1 ethernet and 1 BRI U
c803	Cisco 800 platform with 1 ethernet 4-port hub, 1 BRI S/T, and 2 POTs
c804	Cisco 800 platform with 1 ethernet 4-port hub, 1 BRI U, and 2 POTs
c7206VXR	Cisco 7200 platform, VXR series chassis with 6 slots
c7204VXR	Cisco 7200 platform, VXR series chassis with 4 slots
c1750	VoIP (Voice over IP) capable Cisco 1700 platform with 2 WIC/VIC slots and 1 VIC-only slot
mgx8850	Cisco MGX8850 Multiservice Gigabit Switch with 32 half height slots
c805	Cisco 800 platform with 1 ethernet and 1 serial WIC
ws-c3508g-xl	Cisco Catalyst 3508G-XL switch with 8 GBIC Gigabit ports, can run Standard or Enterprise edition software.
ws-c3512-xl	Cisco Catalyst 3512XL switch with 12 10/100BaseTX ports and 2 GBIC Gigabit ports, can run Standard or Enterprise edition software.

Table 8: Chassis Type (Continued)

Type	Description
ws-c3524-xl	Cisco Catalyst 3524XL switch with 24 10/100BaseTX ports and 2 GBIC Gigabit ports, can run Standard or Enterprise edition software.
ws-c2908-xl	Cisco Catalyst 2900XL series 8 port 10/100BaseTX switch
ws-c2916m-xl	Cisco Catalyst 2916M-XL switch with 16 10/100BaseTX ports and 2 uplink slots.
ws-c2924-xl-v	Cisco Catalyst 2924XL switch with 24 autosensing 10/100BaseTX ports; supports port-based VLANs; can run Standard or Enterprise edition software.
ws-c2924c-xl-v	Cisco Catalyst 2924C-XL switch with 22 autosensing 10/100BaseTX ports and 2 100BaseFX ports; supports port-based VLANs, can run Standard or Enterprise edition software.
ws-c2912-xl	Cisco Catalyst 2912XL switch with 12 autosensing 10/100BaseTX ports, can run Standard or Enterprise edition software.

Table 8: Chassis Type (Continued)

Type	Description
ws-c2924m-xl	Cisco Catalyst 2924M-XL switch with 24 autosensing 10/100BaseTX ports and 2 uplink slots, can run Standard or Enterprise edition software.
ws-c2912mf-xl	Cisco Catalyst 2912MF-XL switch with 12 100BaseFX ports and 2 uplink slots; can only run Enterprise edition software.
c1417	Cisco 1400 series router with 1 Ethernet and 1 ADSL interface, with 1417 chipset
cOpticalRegenerator	Cisco Optical Regenerator
ws-c2924-xl	Cisco Catalyst 2924XL with 24 10/100BaseTX switch ports; doesn't support port-based VLANs.
ws-c2924c-xl	Cisco Catalyst 2924C-XL; doesn't support port-based VLANs.
ubr924	Cisco UBR Cable Modem which is a UBR904 with 2 FXS Voice ports
ws-x6302-msm	Catalyst 6000 or 6500 Series Multilayer Switch Module WS-X6302-MSM that directly interfaces to the switch's backplane to provide layer 3 switching.

Table 8: Chassis Type (Continued)

Type	Description
cat5k-rsfc	Router Switching Feature Card for the Catalyst 5000 that is treated as a standalone system by the NMS
c7120-quadt1	7120 Series chassis with 2 10/100 FE interfaces, 4 T1/E1 interfaces
c7120-t3	7120 Series chassis with 2 10/100 FE interfaces, 1 T3 interface
c7120-e3	7120 Series chassis with 2 10/100 FE interfaces, 1 E3 interface
c7120-at3	7120 Series chassis with 2 10/100 FE interfaces, 1 T3 ATM interface
c7120-ae3	7120 Series chassis with 2 10/100 FE interfaces, 1 E3 ATM interface
c7120-smi3	7120 Series chassis with 2 10/100 FE interfaces, 1 OC3SMI ATM interface
c7140-dualt3	7140 Series chassis with 2 10/100 FE interfaces, 2 T3 interfaces
c7140-duale3	7140 Series chassis with 2 10/100 FE interfaces, 2 E3 interfaces
c7140-dualat3	7140 Series chassis with 2 10/100 FE interfaces, 2 T3 ATM interfaces
c7140-dualae3	7140 Series chassis with 2 10/100 FE interfaces, 2 E3 ATM interfaces

Table 8: Chassis Type (Continued)

Type	Description
c7140-dualmm3	7140 Series chassis with 2 10/100 FE interfaces, 2 OC3MM ATM interfaces
c12016	Cisco 12000 platform with 16 slots
c7140-octt1	7140 Series chassis with 8 integrated T1/E1 serial ports
c7140-dualfe	7140 Series chassis with 2 integrated 10/100 FE interfaces
cat3548xl	Catalyst 3548XL switch (WS-C3548-XL)
mc3810-v3	Cisco MC3810-V3, capable of data, voice and video. Supports 2 additional ports than the MC3810-V, used for optional access cards.
c7507z	Cisco 7507z chassis, Czbus capable, 7 slots
c7513z	Cisco 7513z chassis, Czbus capable, 13 slots
c7507mx	Cisco 7507mx chassis, Czbus capable, TDM (Time Division Multiplexing) backplane support, 7 slots

Table 8: Chassis Type (Continued)

Type	Description
c7513mx	Cisco 7513mx chassis, Czbus capable, TDM Time Division Multiplexing) backplane support, 13 slots
ubr912-c	Cisco uBR912-C Cable Modem with CSU/DSU WIC
ubr912-s	Cisco uBR912-S Cable Modem with Serial WIC
ubr914	Cisco uBR914 Cable Modem with removable WIC
cat4232-l3	Cisco Catalyst 4232-L3 layer 3 line card that is treated as a standalone system by the NMS
cOpticalRegenerator DCPower	Cisco Optical Regenerator with DC power supply
cva122	Cisco CVA122 Cable Voice Adapter (Residential Cable Modem with two Voice Ports)
cva124	Cisco CVA124 Cable Voice Adapter (Residential Cable Modem with four Voice Ports)
ubr7100	A lower end version of the UBR7223, designed for hotels, MDUs and smaller cable operators

Table 8: Chassis Type (Continued)

Type	Description
mgx8240	High Density Circuit Emulation Service Gateway chassis with two shelf controller slots and fifteen Service Modules for Private Line Service
ubr925	Cisco UBR925 Cable Modem/Router with VOIP and hardware accelerated IPSEC
ubr10012	Cisco uBR10000 platform with 8 broadband slots and 4 WAN slots
c12016-8r	Teracore ready 8 rail chassis for Cisco 12000 platform
c2650	c2650 platform with 1 integrated fast ethernet interface
c2651	c2650 platform with 2 integrated fast ethernet interfaces
c626	Cisco 600 DSL CPE platform with ADSL, DMT issue 1, 25M ATM interface
c627	Cisco 600 DSL CPE platform with ADSL, DMT issue 2, 25M ATM interface
c633	Cisco 600 DSL CPE platform with SDSL, 2B1Q line coding, serial interface (V.35/X.21)

Table 8: Chassis Type (Continued)

Type	Description
c673	Cisco 600 DSL CPE platform with SDSL, 2B1Q line coding, ethernet interface
c675	Cisco 600 DSL CPE platform with ADSL, CAP, ethernet interface, POTS connector
c675e	Cisco 600 DSL CPE platform with ADSL, CAP, ethernet interface, universal power supply
c676	Cisco 600 DSL CPE platform with ADSL, DMT issue 1, ethernet interface
c677	Cisco 600 DSL CPE platform with ADSL, DMT issue 2, ethernet interface
c678	Cisco 600 DSL CPE platform with ADSL, CAP/DMT/G.Lite, ethernet interface
c3661-ac	1 Fast Ethernet version of c3660 with a AC power supply
c3661-dc	1 Fast Ethernet version of c3660 with a DC power supply
c3662-ac	2 Fast Ethernet version of c3660 with a AC power supply

Table 8: Chassis Type (Continued)

Type	Description
c3662-dc	2 Fast Ethernet version of c3660 with a DC power supply
c3662-ac-co	2 Fast Ethernet version of c3660 with a AC power supply for Telco's
c3662-dc-co	2 Fast Ethernet version of c3660 with a DC power supply for Telco's
ubr7111	Low-end version of the Universal Broadband Router with 1 PA slot, 1 fixed RF line card (MC11C) and integrated upconvertor, designed for hotels, MDUs and smaller cable operators
ubr7114	Low-end version of the Universal Broadband Router with 1 PA slot, 1 fixed RF line card (MC14C) and integrated upconvertor, designed for hotels, MDUs and smaller cable operators
c12010	Cisco 12000 platform with 10 slots
c8110	Cisco 8110 (ATM network termination device) with 3 Line Interface module slots
c7150-dualfe	7150 Series chassis with 2 integrated 10/100 FE interfaces
c7150-octt1	7150 Series chassis with 8 integrated T1/E1 serial ports

Table 8: Chassis Type (Continued)

Type	Description
c7150-dualt3	7150 Series chassis with 2 10/100 FE interfaces, 2 T3 interfaces
cvps1110	Cisco VLAN Policy Server 1110 manages VLAN-based policies to control user access to a LAN, leveraging existing authentication mechanisms such as Windows Domain Controllers and Novell's NDS. This policy server is part of CiscoWorks2000 User Registration Tool product.
ccontentengine	Cisco Content Engine Chassis. The Cisco Content Engine is a Content Networking product that accelerates content delivery, ensuring maximum scalability and availability of content. The Content Engines offer caching, Content Delivery Network (CDN) services, employee internet management (e.g., URL filtering) and proxy services
ciad2420	Integrated Access Device 2420 (IAD2420) chassis with Analog (8/16) FXS ports with T1 or ADSL (Asymmetrical Digital Subscriber Line) Uplinks

Table 8: Chassis Type (Continued)

Type	Description
c677i	Cisco 600 DSL CPE platform with ASDL, DMT issue 2 over ISDN, ethernet interface
c674	Cisco 600 DSL CPE platform with G.SHDSL, ethernet interface
cdpa7630	The Cisco Digital PBX Adapter (DPA) enables the integration of Cisco Call Manager with Octel voice mail systems
cva122e	Cisco CVA122-e Cable Voice Adapter (Residential Cable Modem with two voice ports)- European version
cva124e	Cisco CVA124-e Cable Voice Adapter (Residential Cable Modem with four voice ports)- European version
curm	Universal Router Module for the IGX platform
curm2fe	Universal router module with 2 Fast Ethernet interfaces for IGX platform
curm2fe2v	Universal Router Module, with 2 Fast Ethernet ports, and 2 digital voice ports (T1 or E1)
cap340	Aironet Wireless LAN Access Point 340 series

Table 8: Chassis Type (Continued)

Type	Description
cdpa7610	The Cisco Digital PBX Adapter (DPA) enables the integration of Cisco Call Manager with Octel voice mail systems
c12416	Cisco 12000 platform with 16 slots and 10G Fabric card
ws-c2948g-l3-dc	A fixed-configuration Layer 3 Ethernet switch featuring IP, IPX, and IP mulitcast with 48 10/100BaseTX ports and 2 GBIC Gigabit ports using DC power
ws-c4908g-l3-dc	A fixed-configuration L3 Ethernet switch featuring IP,IPX and IP multicast with 8 GBIC ports using DC power
c12406	Cisco 12400 platform with 6 slots
pix-firewall506	Cisco PIX Firewall 506
pix-firewall515	Cisco PIX Firewall 515
pix-firewall520	Cisco PIX Firewall 520
pix-firewall525	Cisco PIX Firewall 525
pix-firewall535	Cisco PIX Firewall 535
c12410	Cisco 12410 platform with 10 slots

Table 8: Chassis Type (Continued)

Type	Description
c811	ISDN router for Japan with 1 10BaseT Ethernet port, 1 ISDN BRI (Basic Rate Interface) U, integrated DSU (Data Service Unit)
c813	ISDN router for Japan with 10 BaseT 4 ports hub, 1 ISDN BRI (Basic Rate Interface) U, integrated DSU (Data Service Unit) and 2 RJ-11
c4224	A standalone 24 port powered Ethernet switch, router and voice gateway
c1105	CiscoWorks network management chassis
cCe507	Cisco Content Engine Model 507
cCe560	Cisco Content Engine Model 560
cCe590	Cisco Content Engine Model 590
cCe7320	Cisco Content Engine Model 7320
pix-firewall501	Cisco PIX Firewall 501
c2610M	c2600M chassis with 1 integrated ethernet interface
c2611M	c2600M chassis with 2 integrated ethernet interfaces
c12404	Cisco 12400 platform with 4 slots

Table 8: Chassis Type (Continued)

Type	Description
c9004	Cisco 9000 Chassis
cCe507av	Cisco Content Engine Model 507-AV
cCe560av	Cisco Content Engine Model 560-AV
cIe2105	The Cisco Intelligence Engine 2100 series
c7304	Cisco 7300 Chassis

Chassis ID/Serial No.
A unique identifier for this chassis. The default value is the serial number of the chassis. If no serial number is available and no alternative ID has been set for the chassis, this field will remain empty.

Number of Chassis Slots
The number of slots in this chassis model.

ROM Information
This section of the Chassis General Information view provides the following information about the ROM installed in the chassis:

ROM Monitor Version
The version number of the ROM monitor.

ROM Software Version
The version number of the ROM system software. If no version number is available, this field will remain empty.

Config Register
The current value of the configuration register.

RAM Information
This section of the Chassis General Information view provides the following information about the RAM installed in the chassis:

System CPU RAM (bytes)
The amount of RAM available to the CPU, in bytes.

Non-volatile RAM Used (bytes)
The amount of non-volatile configuration memory in use, in bytes.

Non-volatile RAM Size (bytes)
The total size, in bytes, of non-volatile configuration memory.

Cisco Modem Application

This application (CiscoModemApp) has five menu options that provide access to the following views.

- *Modem System Information View*
- *Modem Line Status Table View* (Page 53)
- *Modem Line Configuration Table View* (Page 57)
- *Modem Line Statistics Table View* (Page 59)
- *Modem Line Speed Statistics Table View* (Page 60)

Modem System Information View

Access: *From the **Icon Subviews** menu for the CiscoModemApp Application icon, select **System Info.***

Installed Modem

The actual number of modems that are currently installed within this system.

Configured Group

The actual number of modem groups that are currently configured within this system.

Watchdog Time

A passive software watchdog timer value will be used to recover a modem that enters into an unexpected state and hangs. When this watchdog timer times out, the modem associated Call Processing state will be set back to “IDLE,” all related Time Division Multiplexing (TDM) paths will be restored to default configurations, and all call processing related actions will stop for the modem.

Status Poll Time

The ideal time interval between modem status polling via the out-of-band management port.

Max Retries

A reply event is expected to be received for every message sent to the modem through the out-of-band management port. If an expected reply event is not received, the message will be sent to the modem again. This object specifies the maximum number of retries that will be executed.

Modems In Use

The number of modems in the system that are in the following states: `connected, offHook, loopback,` or `downloadFirmware`.

Modems Available

The number of modems in the system that are in the onHook state, that is, they are ready to accept a call.

Modems Unavailable

The number of modems in the system that cannot accept calls. These modems are in a state other than the following: `connected, offHook, loopback,` or `downloadFirmware`.

Modems Offline
The number of modems in the system that have been held administratively offline.

Modems Dead
The number of modems in the system with the state equal to `bad` or `downloadFirmwareFailed`.

Modem Line Status Table View

Access: *From the **Icon Subviews** menu for the CiscoModemApp Application icon, select **Line Status Table.***

Slot.Port
The chassis slot and port for this entry.

Interface
The interface to which this modem is connected.

Group
The modem group number that the modem may be in.

Manufacturer ID
A textual description to identify the modem, including the manufacturer's name and type of modem.

Product Details
A textual description of the modem, including hardware revision number, firmware revision number, feature set, and—optionally— its serial number.

Manageable
The Manageable modem allows access through the out of band management port in which the modem statistic data can be retrieved, and the Direct Connect session can be used to provide the test and debugging ability. This object indicates whether this modem is a Manageable modem.

State
Indicates the current state of the modem. The meaning of each state code is explained in the Table 9.

Table 9: Modem States

State	Meaning
unknown	The current state of the modem is unknown.
onHook	The modem is in a state similar to hanging up a telephone receiver. The call cannot enter a connected state when the modem is onHook.
offHook	The modem is in a state similar to picking up a telephone receiver to dial or answer a call.
connected	The modem is in a state where it can transmit or receive data over the communications line.
busiedOut	The modem is busied out (i.e., taken out of service) and cannot make outgoing calls or receive incoming calls.

Table 9: Modem States (Continued)

State	Meaning
disabled	The modem is in a reset state and non-functional. This state can be set and cleared via cmHoldReset.
bad	The modem is suspected or proven to be bad. The operator can take the modem out of service and mark the modem as “bad” via cmBad.
loopback	The modem is in a state where it is currently running back-to-back loopback testing.
downloadFirmware	The modem is in a state where it is currently downloading the firmware.
downloadFirmwareFailed	The modem is not operational because the downloading of firmware to it has failed.

Call Direction

The modem can be used either as an incoming call or outgoing call. This object specifies the direction of the current or previous call.

Disconnect Reason

Indicates the reason that the last connection or call attempt disconnected. The meaning of each reason code is explained in Table 10.

Table 10: Disconnect Reasons

Reason Code	Meaning
unknown	The failure reason is unknown or there has been no previous call.
lostCarrier	The call was disconnected because of the loss of a carrier.
noCarrier	The dial out attempt has failed because the modem detects no carrier.
noDialTone	The dial out attempt has failed because modem failed to detect a dial tone.
busy	The call attempt failed because the modem detected a busy signal.
modemWatchdogTimeout	The modem internal watchdog timer has expired.
dtrDrop	DTR has been turned off while the modem is disconnected on DTR drop.

Table 10: Disconnect Reasons (Continued)

Reason Code	Meaning
userHangup	Normal disconnect where the user hangs up call.
compressionProblem	The call is disconnected due to a problem detected during compression in the modem.
retrainFailure	The modem did not successfully train and reach data mode on the previous connections.
remoteLinkDisconnect	The remote link disconnected the connection.
abort	The call was aborted.
inactivityTimeout	The modem automatically hangs up because data is not sent or received within the inactivity time out.
dialStringError	The dialed phone number is invalid.
linkFailure	The modem detects a link failure.
modulationError	The modem detects a modulation error.
dialTimeout	The modem times out while attempting to dial.

Table 10: Disconnect Reasons (Continued)

Reason Code	Meaning
remoteHangup	The remote side hangs up the connection.
trainupFailure	Failure to train up with a remote peer.
fallbackTerminate	User has EC fallback set to disconnect.
excessiveEC	Link loss due to excessive EC retransmissions.
hostDrop	Host initiated link drop.
terminate	Lost Carrier Microcom HDMS product relating to password security issues.
autoLogonError	An autologon sequence did not complete successfully.
ccpNotSeen	The Credit Card Prompt was not detected.

Table 10: Disconnect Reasons (Continued)

Reason Code	Meaning
callbackFailed	A switched line dialback occurred due to a leased line connection failure, thus the switched line connection also failed and a connection can still not be made on the leased line.
blacklist	In countries that support blacklisting, an attempt was made to go off hook with a null dial string (ATD).
mnp10ProtocolError	MNP10 Protocol Error
lapmProtocolError	LAPM Protocol Error
faxClass2Error	Fax Class 2 Error

Call Duration
This object specifies the call duration of the current or previous call.

Call Phone Number
The dialed outgoing telephone number of the current or previous call.

Caller ID
The incoming caller identification of the current or previous call.

Modulation Scheme Used
The modem modulation scheme used in the current or previous call. This object exists only for modems which have the `cmManageable` object set to "true."

Protocol Used
The modem protocol used in the current or previous call. This object exists only for modems that have the `cmManageable` object set to "true."

TX Rate
The modem transmit rate of the current or previous call in bits per second. This object exists only for modems that have the `cmManageable` object set to "true."

RX Rate
The modem receive rate of the current or previous call in bits per second. This object exists only for modems that have the `cmManageable` object set to "true."

TXAnalog Signal Level
The modem transmit analog signal level in the current or previous call. This object exists only for modems that have the `cmManageable` object set to "true."

RXAnalog Signal Level
The modem receive analog signal level in the current or previous call. This object exists only for modems that have the `cmManageable` object set to "true."

Modem Line Configuration Table View

Access: *From the **Icon Subviews** menu for the CiscoModemApp Application icon, select **Line Config Table.***

This table shows objects that describe configuration information for the modem.

Slot.Port
The chassis slot and port for this entry.

AT Mode Permit
Direct Connect session is used for testing and debugging purposes by using the modem AT commands through the out-of-band management port when cmManageable is set to "true." This object specifies whether the Direct Connect session is permitted to be used at this modem. If cmManageable is "true" (1), Direct Connect session via the out of band port is allowed; if "false" (2), Direct Connect session is not allowed for the modem.

Status Polling
Modem status and events can be polled through the out of band management port when the cmManageable is set to "true." This object specifies whether this status polling feature is

enabled at this modem. If cmManageable is “true” (1), status polling will occur for the modem; if “false” (2) no status polling will occur.

Busy Out Request

This object is used to put the modem out of service, i.e. modem cannot make calls or answer calls. If the modem to be busyout is handling a call, the busyout action will be taken after the current call is disconnected. After the modem is in the busyout state, the following commands can be applied to those modems: reset, bad modem, download modem firmware, etc. This is called “nice” or “graceful” busyout. The value of “true” (1) indicates the busyout request has been issued to the modem, but the busyout could be pending. The management entity needs to query the cmState to see if the modem is successfully busied out. The value of “false” (2) indicates the modem has not been given the busyout command.

Shutdown

This object is used to put the modem out of service — i.e., modem cannot make calls or answer calls. This is a “hard” busyout command to bring the modem out of service immediately without waiting for the call to be ended normally. After the modem is shut down, the following commands can be applied to those modems: reset, bad modem, download modem firmware, etc. The value of “true” (1) indicates the hard busyout has been issued to the modem. The value of “false” (2) indicates the modem has not been given a hard busyout command.

Hold Reset

A command hold-reset will put the state of modem into reset mode until an inverse command is given to bring the modem out of RESET mode. During the period of reset mode, the modem cannot be used. This object is only valid when cmState is onHook, busiedOut, or disabled. The value of “true” (1) attempts to put the modem in reset mode, and the value of “false” (2) takes the modem out of reset.

Bad Modem

This object can hold the modem out of service and marks the modem as suspected or proven to be bad. During the router start-up initialization sequence, modem back-to-back tests will test modems and mark those modems failing tests as bad modems. The management entity also can use this command to lock out the suspect modem or unlock the modem to further debug or test. This object is only valid when cmState is onHook or busiedOut. The value of “true” (1) indicates the modem is suspected to be bad and its state is set to bad. The value of “false” (2) indicates the modem has not been suspected to be bad or has been remarked as good.

Modem Line Statistics Table View

Access: *From the **Icon Subviews** menu for the CiscoModemApp Application icon, select **Line Statistics Table**.*

This table contains objects that describe the status of the modem.

Slot.Port
The chassis slot and port for this entry.

Ring No Answers
The number of calls where ringing was detected but the call was not answered at this modem.

In Connect Failures
The number of incoming connection requests that this modem answered but for which it could not train with the other Data Communications Equipment (DCE). This object exists only for modems that have the `cmManageable` object set to “true.”

In Connect Completions
The number of incoming connection requests that this modem answered and successfully trained with the other DCE. This object exists only for modems that have the `cmManageable` object set to “true.”

Out Connect Failures
The number of outgoing calls from this modem that successfully went off hook and dialed, but for which it could not train with the other DCE. This object exists only for modems that have the `cmManageable` object set to “true.”

Out Connect Completions
The number of outgoing calls from this modem that resulted in successfully training with the other DCE. This object exists only for modems that have the `cmManageable` object set to “true.”

Failed Dial Attempts
The number of call attempts that failed because the modem did not go off hook, or because there was no dial tone.

No Dial Tones
The number of times the dial tone was expected but was not received. This object exists only for modems that have the `cmManageable` object set to “true.”

Dial Timeouts
The number of times the dial time-out occurred. This object exists only for modems that have the `cmManageable` object set to “true.”

Watchdog Timeout
The number of times the Call Processing watchdog timer has expired.

2400 Or Less Connections
The number of connections initially established at a modulation speed of 2400 bits per second or less. This object exists only for modems that have the `cmManageable` object set to “true.”

2400 To 14400 Connections
The number of connections initially established at a modulation speed of greater than 2400 bits per second and less than 14400 bits per second. This object exists only for modems that have the `cmManageable` object set to “true.”

More Than 14400 Connections
The number of connections initially established at a modulation speed of greater than 14400 bits per second. This object exists only for modems that have the `cmManageable` object set to “true.”

No Carriers
The number of times the disconnect reason is no carrier. This object exists only for modems that have the `cmManageable` object set to “true.”

Link Failures
The number of times that the disconnect reason is link failure. The object exists only for modems that have the `cmManageable` object set to “true.”

Protocol Errors
The number of times that the out of band protocol error occurred. This object exists only for modems that have the `cmManageable` object set to “true.”

Polling Timeouts
The number of times that the out of band protocol time-out error occurred. This object exists only for modems that have the `cmManageable` object set to “true.”

Modem Line Speed Statistics Table View

Access: *From the **Icon Subviews** menu for the CiscoModemApp Application icon, select **Line Speed Stats Table**.*

This table displays a collection of objects that describe the initial modem line speeds and connections.

Slot.Port
The chassis slot and port for this entry.

Line Speed
A discrete initial speed at which the given line may operate.

Line Connections
The number of connections initially established at a given modulation speed. An instance of this

object will only be present for those speeds where one or more connections have occurred.

Tx Line Connections

The number of Transmit connections initially established at a given modulation speed. An instance of this object will only be present for those speeds where one or more connections have occurred.

Rx Line Connections

The number of Receive connections initially established at a given modulation speed. An instance of this object will only be present for those speeds where one or more connections have occurred.

Cisco Flash Application

This application (CiscoFlashApp) supports the flash memory used by the Cisco Router. It has eight options that provide access to the following views:

- *Cisco Flash Configuration View* (Page 62)
- *Flash Device Chip Properties Table View* (Page 62)
- *Flash Copy Operations Table View* (Page 63)
- *Flash Device Properties Table View* (Page 65)
- *Flash File Properties Table View* (Page 65)
- *Flash Miscellaneous Operations Table View* (Page 66)
- *Flash Device Partition Properties Table View* (Page 66)
- *Flash Partitioning Operations Table View* (Page 67)

Cisco Flash Configuration View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Flash Configuration**.*

This view provides button access to the other Flash views available from the Icon Subviews menu for the CiscoFlashApp Application. This view also provides the following information.

Flash Size (Bytes)
Total size, in bytes, of flash memory.

Available (Bytes)
Unused size, in bytes, of flash memory.

Flash write
The current write permission is “Disabled” or “Enabled.”

Last Flash Erase
Indicates the value of **sysUptime** the last time Flash memory was erased. If the flash has not been erased since powerup this has a value of `0`.

Flash Directory

This table within the Flash Configuration view provides the following information.

Name
The flash device name.

Size
The total size of the flash device.

Status
The status of the flash device.

Flash Device Chip Properties Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Chip Properties**.*

This view displays the following flash device chip information for each initialized flash device.

Device
The flash device for this entry.

Chip
The flash device chip for this entry.

Description
The flash chip name corresponding to the chip code.

Write Retries
A cumulative count of write retries done on this chip.

Erase Retries
A cumulative count of erase retries done on this chip.

Flash Copy Operations Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Copy Operations**.*

This view displays the following information.

Command
The copy command to be executed.

Protocol
The protocol to be used for any copy. Default is `tftp`.

Server Address
The server address for any copy. Default is `255.255.255.255`.

Source Name
The source file name, either flash or on a server.

Destination Name
The destination address for any copy.

Remote User
The remote user name for copy through rcp protocol.

Copy Status
The status of the specified copy operation.

Notify On Completion
Whether a notification should be generated on the completion of the copy operation.

Entry Status
The status of this table entry.

Add a Copy Operation

This button accesses the Add Flash Copy Operation view which contains the following buttons and fields.

Copy

This button lets you set the copy command for a new copy operation. Possible values are `to flash w/erase`, `to flash w/no erase`, `flash to net`, and `FLH log to server`.

Protocol

This button lets you set the copy protocol for a new copy operation. Possible values are `tftp`, `rcp`, `lex`. The default is `tftp`.

Notify on Completion

This button lets you set whether or not a notification should be generated upon completion of the copy operation.

Server Address
This field lets you set the server address to be used for the copy operation.

Source Filename

This field lets you set the source file name, either in Flash or on a server, depending on the type of copy command.

- For a copy from Flash: File name must be of the form [<device>:][<partition>:]<file> where <device> is a value obtained from FlashDeviceName, <partition> is obtained from FlashPartitionName and <file> is the name of a file in Flash. A management station could derive its own partition name as per the description for ciscoFlashPartitionName. If <device> is not specified, the default Flash device will be assumed. If <partition> is not specified, the default partition will be assumed. If a device is not partitioned into 2 or more partitions, this value may be left out.
- For a copy to Flash: File name will be as per the file naming conventions and path to the file on the server.

Destination Filename

The destination file name.

- For a copy to Flash: File name must be of the form [<device>:][<partition>:]<file> where <device> is a value obtained from FlashDeviceName, <partition> is obtained from FlashPartitionName and <file> is any character string that does not have embedded colon characters. A management station could derive its own partition name as per the description for the ciscoFlashPartitionName object. If <device> is not specified, the default Flash device will be assumed. If <partition> is not specified, the default partition will be assumed. If a device is not partitioned into 2 or more partitions, this value may be left out. If <file> is not specified, it will default to <file> specified in ciscoFlashCopySourceName.
- For a copy from Flash via tftp or rcp, the file name will be as per the file naming conventions and destination sub-directory on the server. If not specified, <file> from the source file name will be used.
- For a copy from Flash via lex, this string will consist of numeric characters specifying the interface on the lex box that will receive the source flash image.

User Name

Remote user name for copy via rcp protocol. This will be ignored for protocols (Page 63) other than rcp. If specified, it will override the remote user-name configured through the rcmd remote-username <username> configuration command. The remote user-name is sent as the server user-name in an rcp command request sent by the system to a remote rcp server.

Add Copy Operation

This button adds the new copy operation to the Flash Copy Operations Table (Page 63).

Flash Device Properties Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Device Properties**.*

This view displays the following information.

Name
The Flash device name.

Partitions
Number of partitions present.

Descriptions
System Flash (primary) and Boot Flash (secondary).

Controller
The card that controls Flash read/write/erase.

Card
Index for the card in the card table.

Jumper
The state of the jumper that controls the programming voltage to the Flash device. Possible values include: `unknown`, where a programming jumper is not present or not required or, `installed` or `not_installed` where the programming jumper state can be read back via a hardware register.

Init Time
The time (system time) the device was initialized.

Flash File Properties Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **File Properties**.*

This view displays the following information for the files in a flash partition.

Name
The name for the file specified by the user copying in the file.

Size
The size of the file in bytes.

Status
The status of the file.

Flash Miscellaneous Operations Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Miscellaneous Operations**.*

This view displays the following information.

Command
The command to be executed.

Destination
The destination file.

Status
The status of the specified operation.

Notify On Completion
Whether a notification should be generated on the completion of the copy operation.

Entry Status
The status of this table entry.

Time
The time taken for the operation.

Flash Device Partition Properties Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Partition Properties**.*

This view displays the following information.

Name
The name for this partition used by the system.

Start Chip
The chip sequence number for the first chip in the partition.

End Chip
The chip sequence number for the last chip in the partition.

Size
The flash partition size.

File Count
The number of files in the partition.

Checksum Algorithm
The identifier for the checksum method used by the file system. When a file system writes a file to flash, it checksums the data written.

Status
Flash partition status. A status of `read_write` indicates the partition is programmable. Other

possible values are `read_only` and `run_from_flash`.

Upgrade Method
The method by which new files can be downloaded into the flash partition. Possible values are `unknown`, `rxbootFLH`, and `direct`. FLH stands for Flash Load Helper, a feature provided on run-from-Flash systems for upgrading Flash. This feature uses the bootstrap code in ROMs to help in automatic download. This field will return `rxbootFLH` if *Status* is `run_from_flash`. If *Status* is `read_only`, the upgrade method would depend on the reason for the `read_only` status. For example, it may require execution of a later version of software that supports the Flash chips.

- `unknown`: the current system image does not know how Flash can be programmed. A possible method would be to reload the ROM image and perform the upgrade manually.
- `rxbootFLH`: the Flash Load Helper is available to download files to Flash. A copy-to-flash command can be used and this system image will automatically reload the Rxboot image in ROM and direct it to carry out the download request.
- `direct`: will be done directly by this image.

Flash Partitioning Operations Table View

Access: *From the **Icon Subviews** menu for the CiscoFlashApp Application icon, select **Partitioning Operations**.*

This view displays the following information.

Command
The partitioning command to be executed.

Destination
The destination device name.

Partition Count
The number of partitions to be created.

Partition Sizes
The size of each partition to be created.

Status
The status of the specified partitioning process.

Notify On Completion
Whether a notification should be generated on the completion of the copy operation.

Entry Status
The status of this table entry.

Time
The time taken for the operation.

Cisco Ping Application

This application (CiscoPingApp) provides access to the Ping Request Table View.

Ping Request Entry View

Access: *From the **Icon Subviews** menu for the CiscoPingApp Application icon, select **Ping Request Entry Table**.*

This view allows you to update the ping request list for this device. The following information is available for this view:

Ping Request Entries

Owner
The user who configured this entry.

Protocol
The protocol to use once an instance of this object is created e.g., Novell, Apple Talk, Vines, etc.

Address
The address of the device to be pinged.

Status
The status of this table entry. Possible states are: `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Pkt Cnt
Specifies the number of ping packets to send to the target device in this sequence.

Pkt Sz
Specifies the size of ping packets to send to the target device in this sequence.

Pkt Timeout
Specifies the amount of time to wait for a response to transmitted packet before declaring the packet dropped.

Delay
Specifies the minimum amount of time to wait before sending the next packet in a sequence after receiving a response or declaring a timeout for a previous packet.

Trap On
Specifies whether or not a ciscoPingCompletion trap should be issued on completion of the sequence of pings.

Pkts Sent
The number of ping packets that have been sent to the target.

Pkts Rcvd
The number of ping packets that have been received from the target in this sequence.

Min RTT
The minimum round trip time in milliseconds of all the packets that have been sent in this sequence.

Avg RTT
The average round trip time in milliseconds of all the packets that have been sent in this sequence.

Max RTT
The maximum round trip time in milliseconds of all the packets that have been sent in this sequence.

Completed
Indicates (true) that all the packets in this sequence have been either responded to or timed out.

Add an Entry

This button opens the Add Ping Request dialog box. Enter the following information and click the **Add Request** button to add an entry to the Ping Request Entry Table:

- Address
- Owner
- Packet Count
- Packet Size
- Packet Timeout
- Delay
- Protocol
- Trap on Completion

Saved Ping Requests

Index
The index for this entry.

Owner
The entity that configured this entry.

Protocol
The protocol to use once an instance of this object is created e.g., Novell, Apple Talk, Vines, etc.

Address
The address of the device to be pinged.

Pkt Cnt
Specifies the number of ping packets to send to the target device in this sequence.

Pkt Sz
Specifies the size of ping packets to send to the target device in this sequence.

Pkt Timeout
Specifies the amount of time to wait for a response to transmitted packet before declaring the packet dropped.

Delay
Specifies the minimum amount of time to wait before sending the next packet in a sequence after receiving a response or declaring a timeout for a previous packet.

Trap On
Specifies whether or not a ciscoPingCompletion trap should be issued on completion of the sequence of pings.

Index to Remove
The index entry that is to be removed.

Log Ping Result?
Set to `true` or `false`. Gives the option of saving the ping result.

This button lets you set the populate interval. Options are `Turn Off Update`, `15 Minutes`, `30 Minutes`, `1 Hour`, `6 Hours`, `12 Hours`, and `1 Day`.

This button lets you clear any saved ping requests.

This button lets you copy saved requests to the device.

Next Ping Will Occur:
The time the next ping will occur.

Click this to view explanations for the buttons in this view.

Cisco Queue Application

This application (CiscoQueueApp) has three menu options that provide access to the information used to manage interface queuing within this device.

- *Queue Interface View*
- *Queue Statistics View*
- *Queue Rotation Interface View* (Page 72)

Queue Interface View

Access: *From the **Icon Subviews** menu for the CiscoQueueApp Application icon, select **Queue Interface**.*

This view provides the following information on the queues for a particular Cisco interface.

IF
The IF index for this interface.

Type
The type of queuing used in the hold queue.

Maximum Number of Msgs
The maximum number of messages placed in the hardware transmission queue.

Number of Sub-Queues
The number of sub-queues from which the hold queue is built.

Queue Statistics View

Access: *From the **Icon Subviews** menu for the CiscoQueueApp Application icon, select **Queue Statistics**.*

This view provides the following statistical information on the queues for a particular Cisco interface.

IF Index
The IF index for this interface.

Queue
The number of the queue within the queue set. In FIFO queuing, this value is always 2. In Priority Queuing, it corresponds to the various priorities shown in Table 11.

Table 11: Queuing Priorities

Value	Priority
0	high
1	medium
2	normal
3	low

In Custom Queuing, it is the queue number referenced in the access list. In Weighted Fair

Queuing, it is the queue number associated with the traffic stream (conversation) identified.

Number of Msgs
The number of messages in the sub-queue.

Max Permitted Msgs
The maximum number of messages permitted in the sub-queue.

Discarded Msgs
The number of messages discarded from this queue since restart.

Queue Rotation Interface View

Access: *From the **Icon Subviews** menu for the CiscoQueueApp Application icon, select **Rotation Interface**.*

This view provides the following information on the rotation of custom queues for a particular Cisco interface.

Statistics Queue Number
Custom queuing sub-queue attributes for an interface.

Number of Transmitted Octets
The number of octets that may be transmitted from a custom queuing sub-queue before it must yield to another queue.

ATM Client Application

This application (**ATMClientApp**) has four menu options that provide access to the following views:

- *VCL Table*
- *ATM Link Modeling Options* (Page 74)

VCL Table

Access: *From the **Icon Subviews** menu for the ATMClientApp Application icon, select **VCL Table.***

This view opens the ATM Client Application Virtual Channel Link (VCL) view with the following information.

If Index
An entry in the VCL Table.

VPI
The Virtual Path Identifier (VPI) value of the VCL.

VCI
The Virtual Channel Identifier (VCI) value of the VCL.

Admin Status
This object is implemented only for a VCL that terminates a VCC (i.e., one that is not cross-connected to other VCLs). Its value specifies the desired administrative state (up or down) of the VCL.

Oper Status
This object indicates the current operational status (up, down, or unknown) of the VCL.

Last Change
The value of MIB II's System Up Time object at the time this VCL entered its current operational state. If the current state was entered prior to the last re-initialization of the agent, then this object contains a zero value.

Rcv Descr Index
The value of this object identifies the row in the ATM Traffic Descriptor Table that applies to the receive direction of this VCL.

Xmit Descr Index
The value of this object identifies the row of the ATM Traffic Descriptor Table that applies to the transmit direction of this VCL.

AAL Type
The type of AAL used on this VCC. An instance of this object only exists when the local VCL endpoint is also the VCC endpoint, and AAL is in use.

Transmit Size
The maximum AAL5 CPCS SDU size in octets that is supported on the transmit direction of this VCC. An instance of this object only exists when the local VCL end-point is also the VCC endpoint, and AAL5 is in use.

Receive Size
The maximum AAl5 CPCS SDU size in octets that is supported on the receive direction of this VCC. An instance of this object only exists when the local VCL end-point is also the VCC endpoint, and AAL5 is in use.

Encaps Type
The type of data encapsulation used over the AAL5 SSCS layer. An instance of this object only exists when the local VCL endpoint is also the VCC end-point, and AAL5 is in use.

Cross Connect Id
This object is implemented only for a VCL that is cross-connected to other VCLs that belong to the same VCC.

Row Status
This object is used to create, delete, or modify a row in this table. To create a new VCL, this object is initially set to "createAndWait" or "createAndGo."

Row Status Procedure
This procedure provides step-by-step instructions to create or remove channel information.

ATM Link Modeling Options

Access: *From the **Icon Subviews** menu for the ATMClientApp Application icon, select **ATM Link Modeling Options.***

This view provides you with a means to create a model for each VCL and VPL configured on this device. Use the **Create Link Models** button to customize how models are created or destroyed for the device. Normally, both VPL and VCL models are created at the same time when the device is configured. This view gives you the option of creating VPL, VCL, or both models as needed.

Setting the **Create Link Models** button and the **Create VCL Models** button to `True` causes SPECTRUM to create both VCL and VPL models. You may set the **Config Interval** field in order to set the intervals between link configurations. If the **Create Link Model** button is set to `False`, neither model will be created. This view contains the following information.

Create Link Models

This button can be set to either true or false. Setting this button's value to `true` causes a model to be created for the VPLs.

Create VCL Models

This button can be set to either true or false. Setting this button's value to `true` causes a model to be created for the VCLs.

Config Interval

This value represents the number of seconds between link model configuration.

Reconfigure Now

Clicking this button forces a link model reconfiguration.

Option Explanations

Clicking this button will display information on the buttons and fields in this view and show you how to force a link model reconfiguration.

Below are detailed instructions on how to create and destroy VCL and VPL models.

Creating VPL/VCL Models

1. Model the device that contains the ATM application.
2. Proceed to the Application view and find the ATM application icon.
3. Right-click the icon and select **ATM Link Modeling Options.** You may select the **Option Explanations** button to display instructions on screen.
4. Set both **Create Link Models** and **Create VCL Models** buttons to `True`. Save the change.
5. Click the **Reconfigure Now** button. This will create both VPL and VCL models.

Note: If you set **Create Link Models** to `True` but **Create VCL Models** to `False`, VCL models will not be created during the reconfiguration.

6. Launch your Device Topology view.
7. Locate the port number associated with the ATM application.
8. Go to the port's Sub-Interface view. You will see the VPL/VCL models after the reconfiguration is completed.

Destroying VPL/VCL Models

1. In the ATM Link Modeling Options view set the **Create Link Models** button to `False`.
2. Save the changes.
3. Click the **Reconfigure Now** button. The VPL/VCL models will be destroyed during the reconfiguration.
4. Launch the Device Topology view.
5. Locate the port associated with the ATM Application.

Go to the Sub-Interface view of the port. You should not see the VPL/VCL models after the reconfiguration is completed.

EnvMon Application

This application (CiscoEnvMonApp) has five menu options that provide access to the following views:

- *Enable Notifications*
- *Fan Status*
- *Power Supply Status* (Page 77)
- *Temperature Status* (Page 77)
- *Voltage Status* (Page 77)

Enable Notifications

Access: *From the **Icon Subviews** menu for the CiscoEnvMonApp Application icon, select **Enable Notifications**.*

This view allows you to enable or disable system notifications.

Present
The type of environmental monitor located in the chassis. Possible values are `oldAgs`, `ags`, `c7000`, `ci`, `cAccessMon`, `cat6000`, `ubr7200`, or `cat4000`.

Shutdown
This button indicates whether the system produces the Shutdown Notification.

Voltage
This button indicates whether the system produces the Voltage Notification.

Redundant Supply
This button indicates whether the system produces the Redundant Supply Notification.

Temperature
This button indicates whether the system produces Temperature Notification.

Fan
This button indicates whether the system produces the Fan Notifications.

Fan Status

Access: *From the **Icon Subviews** menu for the CiscoEnvMonApp Application icon, select **Fan Status**.*

This table provides the fan status maintained by the environmental monitor. The **Description** identifies the fan being instrumented and the **State** identifies the current state of the fan being instrumented.

Power Supply Status

Access: *From the **Icon Subviews** menu for the CiscoEnvMonApp Application icon, select **Power Supply Status**.*

This table provides the power supply status maintained by the environmental monitor card. The **Description** identifies the power supply being instrumented and the **State** identifies the current state of the power supply being instrumented.

Temperature Status

Access: *From the **Icon Subviews** menu for the CiscoEnvMonApp Application icon, select **Temperature Status**.*

This table provides the ambient temperature status maintained by the environmental monitor.

Description
The testpoint being instrumented.

Value
The current measurement of the testpoint being instrumented.

Threshold
The highest value that the associated instance of the object Status Value may obtain before an emergency shutdown of the managed device is initiated.

@ Last Shutdown
The value of the associated instance of the object Status Value at the time an emergency shutdown of the managed device was last initiated. This value is stored in non-volatile RAM and is therefore able to survive the shutdown.

State
The current state of the testpoint being instrumented.

Voltage Status

Access: *From the **Icon Subviews** menu for the CiscoEnvMonApp Application icon, select **Voltage Status**.*

This table provides the voltage status maintained by the environmental monitor.

Description
The testpoint being instrumented.

Value
The current measurement of the testpoint being instrumented.

Lo Threshold
The lowest value that the associated instance of the object Voltage Status Value may obtain before

an emergency shutdown of the managed device is initiated.

Hi Threshold
The highest value that the associated instance of the object Voltage Status Value may obtain before an emergency shutdown of the managed device is initiated.

@ Last Shutdown
The value of the associated instance of the object Voltage Status Value at the time an emergency shutdown of the managed device was last initiated. This value is stored in non-volatile RAM and hence is able to survive the shutdown.

State
The current state of the testpoint being instrumented.

Discovery Application

This application (CiscoCDPApp) has two menu options that provide access to the following views.

- *Discovery Cache Table View*
- *Interface Discovery Status Table* (Page 79)

Discovery Cache Table View

Access: *From the **Icon Subviews** menu for the CiscoCDPApp Application icon, select **Cache**.*

This table contains the cached information obtained by receiving Cisco Discovery Protocol (CDP) messages.

Type
An indication of the type of address contained in the corresponding instance of `cdpCacheAddress`.

Address
The (first) network-layer address of the device's SNMP-agent as reported in the most recent CDP message.

Device ID
The Device-ID string as reported in the most recent CDP message. The zero-length string indicates no Device-ID field was reported in the most recent CDP message.

Device Port
The Port-ID string as reported in the most recent CDP message. This will typically be the value of the ifName object (e.g., 'Ethernet0'.) The zero-length string indicates no Port-ID field was reported in the most recent CDP message.

Platform
The device's hardware platform as reported in the most recent CDP message. The zero-length string indicates that no Platform field was reported in the most recent CDP message.

Capabilities
The device's functional capabilities as reported in the most recent CDP message. For the latest set of specific values, see the latest version of the CDP specification. The zero-length string indicates no Capabilities field was reported in the most recent CDP message.

Interface Discovery Status Table

Access: *From the **Icon Subviews** menu for the CiscoCDPApp Application icon, select **Interfaces.***

This table contains the status of Cisco Discovery Protocol (CDP) on the device's interfaces.

IF
The interface index value of the local interface.

Discovery
An indication of whether the Cisco Discovery Protocol is currently running on this interface.

Group
This object is only relevant to interfaces that are repeater ports on 802.3 repeaters; it indicates the RFC1516 group number of the repeater port that corresponds to this interface.

Port
This object is only relevant to interfaces that are repeater ports on 802.3 repeaters; it indicates the RFC1516 port number of the repeater port that corresponds to this interface.

Interval
The interval at which CDP (Cisco Discovery Protocol) messages are to be generated on this interface. The default value is 60 seconds.

Cisco Interface Application

Access: *From the **Icon Subviews** menu for the CiscoIfApp icon, select **Configuration**.*

This application (CiscoIfceApp) provides access to the application-specific CiscoIfceApp Configuration view, described below.

CiscoIfceApp Configuration

Note: By default, CiscoIfceApps will not be modeled. After changing either setting below, reconfigure the applications.

The following buttons control whether or not CiscoIfceApps will be modeled.

Create Interface Applications

To create CiscoIfceApps for physical interfaces, set this button to `true`.

Create Sub Interface Applications

To create CiscoIfceApps for all interfaces, set this button to `true`.

Cisco Terminal Server Application

The Cisco Terminal Server Application (CiscoTSApp) has three menu options that provide access to the following views:

- *Line Configuration View*
- *Cisco Terminal Server Line View* (Page 81)
- *Cisco Terminal Server Session View* (Page 82)

Line Configuration View

Access: *From the **Icon Subviews** menu for the CiscoTSApp Application icon, select **Line Configuration.***

This view displays the following information on the terminal server lines.

Lines
Number of lines.

Message tty Line
The tty line to send the message to.

Message Interval time
The interval in milliseconds between reissuing message.

Message Duration
The length of time in milliseconds to reissue message.

Message Text
The actual message, up to 256 characters.

Message Temporary Banner
Select to use the message as a temporary banner in addition to the normal banner.

Message send
The value used to determine what is done after the message is sent.

Clear tty Line
The last line cleared.

Cisco Terminal Server Line View

Access: *From the **Icon Subviews** menu for the CiscoTSApp Application icon, select **Line Table.***

This view displays the following information on each terminal server line connected to the Cisco Router.

Status
The current state of this line. Possible states are: `Active` and `Inactive`.

Type
The type of line. Possible types are: `Unknown`, `Console`, `Terminal`, `Line-Printer`, `Virtual-Terminal`, and `Auxiliary`.

Autobaud
Indicates whether or not the line will autobaud.

Speed In
The input speed of this line, displayed as a baud rate.

Speed Out
The output speed of this line, displayed as a baud rate.

Flow Control
The type of flow control in use on this line. Possible flow control types are: `Unknown`, `None`, `Software-Input`, `Software-Output`, `Software-Both`, `Hardware-Input`, `Hardware-Output`, and `Hardware-Both`.

Modem Control
The type of modem control in use on this line. Possible modem control types are: `Unknown`, `None`, `Call-In`, `Call-Out`, `CTS-Required`, `RI-IS-CD`, and `InOut`.

Location
The physical location of this line.

Term Type
The type of terminal on this line.

Length in Lines
Length, in lines, of the terminal screen attached to this line.

Width in Char
Width, in characters, of the terminal screen attached to this line.

Escape Char
Escape character used to breakout the active sessions.

Idle Time out
The amount of idle time allowed on this line before the line times out.

Session Time out
The amount of idle time allowed in this session before the session times out.

Rotary
The rotary group number the line belongs to.

# of Connections
The number of times a connection has been made to or from this line.

Current Session
The current number of sessions in use on this line.

User
Terminal Access Controller Access Control System (TACACS) user name, if TACACS is enabled.

Noise
Count of garbage characters received when the line is inactive.

Line Number
The number (listed in sequential order) for this terminal server line.

Time Active
The time, in seconds, since the line was activated.

Cisco Terminal Server Session View

Access: *From the **Icon Subviews** menu for the CiscoTSApp Application icon, select **Session Table.***

This view displays the Terminal Server (TS) Session Table, which provides information about each terminal server session connected to the Cisco Router.

Type
Identifies session type as `Pad, Stream, Rlogin, Telnet, TCP` and `Unknown`.

Direction
The direction of this session. Possible directions are: `Unknown, Incoming`, and `Outgoing`.

Addr
The remote host address of the session.

Name
The remote host name of the session.

State
Indicates whether this session is the currently "Active" or "Inactive."

Idle
Time in seconds that the session has been idle.

Line
The index value that identifies this line.

Session
A second index value that identifies this session.

Cisco Memory Pool Application

This application (Cisco_Mem_App) provides the *Cisco Memory Pool Monitor Table View*, described below.

Cisco Memory Pool Monitor Table View

Access: *From the **Icon Subviews** menu for the Cisco_Mem_App icon, select **Memory Pool Monitor.***

This table displays memory pool monitoring entries.

Name
Displays the name assigned to a memory pool.

Alternate
Indicates whether or not this memory pool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If this has a value of zero then there is no alternate.

Valid
This indicates whether or not the remaining objects in this entry contain accurate data. If an instance of this object has a false value, the

values of this row may contain inaccurate information.

Used
Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.

Free
The number of bytes from the memory pool that are currently unused on the managed device.

Largest Free
Indicates the largest number of contiguous bytes from the memory pool that are currently unused on the managed device.

Cisco Syslog Application

See *Syslog Trap Support* (Page 166) for more information about this application. The Cisco Syslog Application provides access to the following views:

- *Cisco Syslog Message Filter View*
- *Cisco SysLog Basic Configuration View* (Page 85)
- *Cisco SysLog History Table View* (Page 86)

Cisco Syslog Message Filter View

Access: *From the **Icon Subviews** menu of the CiscSysLogApp icon, select **Syslog Message Filters**.*

This view allows you to filter out unwanted syslog messages and prevent the creation of alarms or events from unwanted messages. Filters can be set to `true` or `false`.

System_Filter
Set to `true` to filter out all Syslog messages whose Facilities deal with the System, e.g. CBUS, MEMSCAN, etc.

Protocol_Filter
Set to `true` to filter out all Syslog messages whose facilities deal with Protocols such as BGP, OSPF, SNMP, SPANTREE, etc.

Software_Filter
Set to `true` to filter out all Syslog messages that deal with internal software such as PARSER, RSP, GRPGE, etc.

Hardware_Configuration_Filter
Set to `true` to filter out all Syslog messages that deal with Hardware Configuration of the device such as IOCARD, MODEM, DIALSHELF, etc.

Security_Filter
Set to `true` to filter out all Syslog messages that deal with the Security of the system such as RADIUS, SECURITY, etc.

Environment_Filter
Set to `true` to filter out all Syslog messages that deal with Environment variables such as LCFE, LCGE, etc.

Connection_Configuration_Filter
Set to `true` to filter out all Syslog messages that deal with Connection Configuration of the device such as MROUTE, ISDN, X25, etc.

Pix_Firewall_Filter
Set to `true` to filter out all Syslog Messages that deal with the Cisco PIX Firewall device.

Cisco SysLog Basic Configuration View

Access: *From the **Icon Subviews** of the CiscSysLogApp Application icon, select **Basic**.*

This view displays the following information.

Notifications Sent
The number of syslog Message Generated notifications that have been sent. This number may include notifications that were prevented from being transmitted due to reasons such as resource limitations and/or non-connectivity. If one is receiving notifications, one can periodically poll this object to determine if any notifications were missed. If so, a poll of the History Table may be appropriate.

Notifications Enabled
Indicates whether notifications will or will not be sent when a syslog message is generated by the device. Disabling notifications does not prevent syslog messages from being added to the History Table.

Messages Ignored
Indicates the number syslog messages which were ignored. A message will be ignored if it has a severity value greater then Max Severity.

Messages Dropped
The number of messages which could not be processed due to a lack of system resources. A message that is dropped will not appear in the History Table.

Max Severity Level
Indicates which syslog severity levels will be processed. Any syslog message with a severity value greater than this value will be ignored by the agent. Severity numeric values increase as their severity decreases, e.g. error (4) is more severe than debug (8). Severity values are (1) emergency, (2) alert, (3) critical, (4) error, (5) warning, (6) notice, (7) info, and (8) debug.

Cisco SysLog History Table View

Access: *From the **Icon Subviews** of the CiscSysLogApp Application icon, select **History**.*

This view displays the History Table which displays the syslog messages generated by the device.

Max Table Length
The limit on the number of entries that the History Table may contain. A value of 0 will prevent any history from being retained. When this table is full, the oldest entry will be deleted and a new one will be created.

Messages Flushed
The number of entries that have been removed from the History Table in order to make room for new entries. This object can be used to determine whether your polling frequency is fast enough.

Index
An increasing integer that indexes messages. When it reaches the maximum value, the agent flushes the table and returns this value to 1.

Facility
The name of the facility that generated this message.

Severity
The severity of the message.

Message Name
A textual name for the message type. A facility name in conjunction with a message name uniquely identifies a message type.

Message Text
The text of the message. If the text of the message exceeds 255 bytes, the message will be truncated to 254 bytes and a '*' character will be appended to indicate this.

Time Stamp
The value of sysUpTime when this message was generated.

Cisco IPM Routing Application

This application (CiscIPMRoutApp) provides the following IP multicasting management views:

- *IPM Route Table View*
- *IPM Route Next Hop Table View* (Page 88)
- *IPM Route Interface Table View* (Page 90)
- *IPM Route Boundary Table View* (Page 90)
- *Cisco IPM Route Table View* (Page 91)
- *Cisco IPM Route Next Hop Table View* (Page 93)
- *Cisco IPM Route Heartbeat Table View* (Page 94)

IPM Route Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Route**.*

This view provides the IPM Route table as well as an *IPM Route Enable* (Page 88) button, both described below.

IPM Route Table

This table contains the following IP multicast routing information.

Group Address
The IP multicast group address for which this entry contains multicast routing information.

Source Address
The network address which when combined with the corresponding value of **Source Mask** (Page 87) identifies the sources for which this entry contains multicast routing information.

Source Mask
The network mask which when combined with the corresponding value of **Source** (Page 87) identifies the sources for which this entry contains multicast routing information.

Upstream Neighbor
The address of the upstream neighbor (e.g., RPF neighbor) from which IP datagrams from these sources to this multicast address are received, or 0.0.0.0 if the upstream neighbor is unknown (e.g., in CBT).

IF Index
The value of **IF Index** for the interface on which IP datagrams sent by these sources to this multicast address are received. A value of 0 indicates that datagrams are not subject to an incoming interface check, but may be accepted on multiple interfaces (e.g., in CBT).

Up Time
The time since the multicast routing information represented by this entry was learned by the router.

Expiry Time
The minimum amount of time remaining before this entry will be aged out. The value 0 indicates that the entry is not subject to aging.

Packets
The number of packets which this router has received from these sources and addressed to this multicast group address.

Diff In IF Packets
The number of packets which this router has received from these sources and addressed to this multicast group address, which were not received from the interface indicated by **IF Index** (Page 87).

Octets
The number of octets contained in IP datagrams which were received from these sources and addressed to this multicast group address, and which were forwarded by this router.

Protocol
The routing mechanism via which this route was learned. Possible values are `other`, `local`, `netmgmt`, `dvmrp`, `mospf`, `pimSparseDense`, `cbt`, `pimSparseMode`, `pimDenseMode`, and `igmpOnly`.

IPM Route Enable

This button lets you enable and disable IP multicast routing.

IPM Route Next Hop Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Route Next Hop**.*

This view provides the IPM Route Next Hop table, described below.

IPM Route Next Hop Table
This table contains the following information on the next hops on outgoing interfaces for routing IP multicast datagrams. Each entry is one of a list of next hops on outgoing interfaces for particular sources sending to a particular multicast group address.

Group
The IP multicast group for which this entry specifies a next hop on an outgoing interface.

Source
The network address which when combined with the corresponding value of **Source Mask**

identifies the sources for which this entry specifies a next hop on an outgoing interface.

Source Mask
The network mask which when combined with the corresponding value of **Source** (Page 88) identifies the sources for which this entry specifies a next hop on an outgoing interface.

IF Index
The **IF Index** value of the interface for the outgoing interface for this next hop.

Address
The address of the next hop specific to this entry. For most interfaces, this is identical to **Group** (Page 88). NBMA interfaces, however, may have multiple next hop addresses out a single outgoing interface.

State
An indication of whether the outgoing interface and next hop represented by this entry is currently being used to forward IP datagrams. The value `forwarding` indicates it is currently being used while the value `pruned` indicates that it is not.

Up Time
The time since the multicast routing information represented by this entry was learned by the router.

Expiry Time
The minimum amount of time remaining before this entry will be aged out. The value `0` indicates that the entry is not subject to aging.

Closest Member Hops
The minimum number of hops between this router and any member of this IP multicast group reached via this next hop on this outgoing interface. Any IP multicast datagrams for the group which have a TTL less than this number of hops will not be forwarded to this next hop.

Protocol
The routing mechanism via which this next-hop was learned. Possible values are `other`, `local`, `netmgmt`, `dvmrp`, `mospf`, `pimSparseDense`, `cbt`, `pimSparseMode`, `pimDenseMode`, and `igmpOnly`.

Packets
The number of packets which have been forwarded using this route.

IPM Route Interface Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Route Interface**.*

This view provides the IPM Route Interface table, described below.

IPM Route Interface Table

This table contains the following multicast routing information specific to interfaces. Double-clicking any entry in this table opens the IPM Route Interface Table Entry view, which displays information for and lets you configure that entry.

IF Index
The **IF Index** value of the interface for which this entry contains information.

TTL Threshold
The datagram TTL threshold for the interface. Any IP multicast datagrams with a Time to Live less than this threshold will not be forwarded out the interface. The default value of `0` means all multicast packets are forwarded out the interface.

Protocol
The routing protocol running on this interface. Possible values are `other`, `local`, `netmgmt`, `dvmrp`, `mospf`, `pimSparseDense`, `cbt`, `pimSparseMode`, `pimDenseMode`, and `igmpOnly`.

Rate Limit
The rate-limit, in kilobits per second, of forwarded multicast traffic on the interface. A rate-limit of `0` indicates that no rate limiting is done.

In Mcast Octets
The number of octets of multicast packets that have arrived on the interface.

Out Mcast Octets
The number of octets of multicast packets that have been sent on the interface.

IPM Route Boundary Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Route Boundary**.*

This view provides the IPM Route Boundary table, described below.

IPM Route Boundary Table

This table lists the router's scoped multicast address boundaries and contains the following information.

IF Index
The **IF Index** value for the interface to which this boundary applies. Packets with a destination address in the associated address/mask range will not be forwarded out this interface.

Address
The group address which when combined with the corresponding value of **Address Mask** identifies the group range for which the scoped boundary exists. Scoped addresses must come from the range 239.x.x.x.

Address Mask
The group address mask which when combined with the corresponding value of **Address** identifies the group range for which the scoped boundary exists.

Status
The status of this row, by which new entries may be created, or old entries deleted from this table. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Cisco IPM Route Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Cisco Route**.*

This view provides the Cisco IPM Route table, described below.

Cisco IPM Route Table

This table contains multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router. This table augments the *IPM Route Table* (Page 87) and contains the following information.

Group Address
The IPM Route **Group Address**, described on Page 87.

Source Address
The IPM Route **Source Address**, described on Page 87.

Source Mask
The IPM Route **Source Mask**, described on Page 87.

Prune Flag
A Boolean value of `true` or `false` indicating whether this route is pruned. A pruned route is one that has an empty outgoing interface list or all interfaces are in `pruned` *State* (Page 89). A

multicast packet that matches a pruned route doesn't get forwarded.

Sparse Flag
A Boolean value of `true` or `false` indicating PIM multicast routing protocol **sparse-mode** (versus **dense-mode)**. In sparse-mode, packets are forwarded only out interfaces that have been joined. In dense-mode, they are forwarded out all interfaces that have not been pruned (see Page 91).

Connected Flag
A Boolean value of `true` or `false` indicating whether there is a directly connected member for a group attached to the router.

Local Flag
A Boolean value of `true` or `false` indicating whether the local system is a member of a group on any interface.

Register Flag
This Boolean value of `true` or `false` indicates whether to send registers for the entry. A first hop router directly connected to a multicast source host, as well as a border router on the boundary of two domains running different multicast routing protocols, encapsulates packets to be sent on the shared tree. This is done until the **RP** sends **Joins** back to this router.

RP Flag
A Boolean value of `true` or `false` indicating whether there is a **Prune** state for this source along the shared tree.

SPT Flag
A Boolean value of `true` or `false` indicating whether data is being received on the SPT tree, i.e. the Shortest Path Tree.

Bits/Second
Bits per second forwarded by this router. This is the sum of all forwarded bits during a 1 second interval. At the end of each second the field is cleared.

Metric
The best metric heard from Assert messages. The value of **Metric2** (Page 93) is used to correctly represent a 32-bit unsigned metric value.

Metric Preference
The best metric preference heard from Assert messages.

In Limit
Incoming interface's limit for rate limiting data traffic, in Kbps. Replaced by *In Limit2* (Page 93).

Last Used
Time since the last multicast packet was fastswitched.

In Limit2
Incoming interface's limit for rate limiting data traffic, in Kbps.

Join Flag
This Boolean value of `true` or `false` indicates whether this route is created due to SPT threshold.

MSDP Flag
This Boolean value of `true` or `false` indicates whether this route is learned via MSDP.

Proxy Join Flag
This Boolean value of `true` or `false` indicates whether to send join for this entry.

Metric2
The best metric heard from Assert messages.

Cisco IPM Route Next Hop Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Cisco Route Next Hop**.*

This view provides the Cisco IPM Route Next Hop table, described below.

Cisco IPM Route Next Hop Table

This table contains information on the next hops on outgoing interfaces for routing IP multicast datagrams. Each entry is one of a list of next hops on outgoing interfaces for particular sources sending to a particular multicast group address.

Group Address
The IPM Route **Group Address**, described on Page 87.

Source Address
The IPM Route **Source Address**, described on Page 87.

Source Mask
The IPM Route **Source Mask**, described on Page 87.

IF Index
The **IF Index** value of the interface for the outgoing interface for this next hop.

Address
The address of the next hop specific to this entry. For most interfaces, this is identical to **Group** (Page 88). NBMA interfaces, however, may have multiple next hop addresses out a single outgoing interface.

Outgoing Limit
An outgoing interface's limit for rate limiting data traffic, in Kbps.

MAC Address Header
The data link mac address header for a multicast datagram. This value is used by IP multicast fastswitching.

Cisco IPM Route Heartbeat Table View

Access: *From the **Icon Subviews** menu for the CiscIPMRoutApp Application icon, select **Cisco Route Heart Beat**.*

This view provides the Cisco IPM Route Heart Beat table, described below.

Cisco IPM Route Heart Beat Table

This table lists sets of IP Multicast heartbeat parameters. If no IP Multicast heartbeat is configured, this table would be empty. This table contains the following information.

Group Address
Multicast group address used to receive heartbeat packets.

Source Address
Source address of the last multicast heartbeat packet received.

Interval
Number of seconds in which a Cisco multicast router expects a valid heartBeat packet from a source. This value must be a multiple of 10.

Window Size
Number of **Interval** intervals a Cisco multicast router waits before checking if expected number of heartbeat packets are received or not.

Count
Number of time intervals where multicast packets were received in the last **Window Size** intervals.

Minimum
The minimum number of heartbeat packets expected in the last **Window Size** intervals. If **Count** falls below this value, an SNMP trap/notification, if configured, will be sent to the NMS.

Alert Time
The value of sysUpTime on the most recent occasion at which a missing IP multicast heartbeat condition occurred for the group address specified in this entry. If no such condition has occurred since the last re-initialization of the local management subsystem, this field contains a zero value.

Row Status
Used to create a new row or delete an existing row in this table. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Cisco PIM Application

This application (CiscoPIMApp) provides the following Protocol Independent Multicast (PIM) management views:

- *PIM Interface Table View* (Page 96)
- *PIM Neighbor Table View* (Page 97)
- *PIM IPM Route Table View* (Page 97)
- *PIM Rendezvous Point Sets Table View* (Page 98)
- *PIM IPM Route Next Hop Table View* (Page 99)
- *PIM Candidate Rendezvous Point Table View* (Page 100)
- *PIM Component Table View* (Page 101)
- *Cisco PIM Objects View* (Page 102)

PIM Interface Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Interface**.*

This view provides the PIM Interface table as well as an additional, user-configurable **Join Prune Interval** field, both described below.

PIM Interface Table

This table lists the router's PIM interfaces. IGMP and PIM are enabled on all interfaces listed in this table. Double-clicking any entry in the PIM Interface table opens the PIM Interface Table Entry view, which displays PIM Interface information for and allows configuration of that entry. The PIM Interface table contains the following information.

IF Index
The **IF Index** value of this PIM interface.

Address
The IP address of the PIM interface.

Net Mask
The network mask for the IP address of the PIM interface.

Mode
The configured mode of this PIM interface. A value of `sparseDense` is only valid for PIMv1. Possible values are `dense`, `sparse`, and `sparseDense`. You can set this value in the PIM Interface Table Entry view (Page 96).

Designated Rtr
The Designated Router on this PIM interface. For point-to-point interfaces, this field has the value 0.0.0.0.

Hello Interval
The frequency at which PIM Hello messages are transmitted on this interface. You can set this value in the PIM Interface Table Entry view (Page 96).

Status
The status of this entry. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`. Creating the entry enables PIM on the interface; destroying the entry disables PIM on the interface. You can set this value in the PIM Interface Table Entry view (Page 96).

Join Prune Interval
The frequency at which PIM Join/Prune messages are transmitted on this PIM interface. You can set this value in the PIM Interface Table Entry view (Page 96), or in the **Join Prune Interval** field below the PIM Interface table.

CBSR Preference
The preference value for the local interface as a candidate bootstrap router. A value of `-1` is used to indicate that the local interface is not a candidate BSR interface. You can set this value in the PIM Interface Table Entry view (Page 96).

PIM Neighbor Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Neighbor**.*

This view provides the PIM Neighbor table, described below.

PIM Neighbor Table

This table lists the router's PIM neighbors and contains the following information.

IP Address
The IP address of the PIM neighbor for which this entry contains information.

IF Index
The value of **IF Index** for the interface used to reach this PIM neighbor.

Up Time
The time since this PIM neighbor (last) became a neighbor of the local router.

Expiry Time
The minimum time remaining before this PIM neighbor will be aged out.

Mode
The active PIM mode of this neighbor. This field is deprecated for PIMv2 routers since all neighbors on the interface must be either dense or sparse as determined by the protocol running on the interface. Possible values are `dense` and `sparse`.

PIM IPM Route Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **PIM IPM Route**.*

This view provides the PIM IPM Route table, described below.

PIM IPM Route Table

This table lists PIM-specific information on a subset of the rows of the *IPM Route Table* (Page 87) and contains the following information.

Group Address
The value of **Group Address** from the IPM Route Table (Page 87).

Source Address
The value of **Source Address** from the IPM Route Table (Page 87).

Source Mask
The value of **Source Mask** from the IPM Route Table (Page 87).

Upstream Assert Time
The time remaining before the router changes its upstream neighbor back to its RPF neighbor. This timer is called the Assert timer in the PIM Sparse and Dense mode specification. A value of `0` indicates that no Assert has changed the upstream neighbor away from the RPF neighbor.

Assert Metric
The metric advertised by the assert winner on the upstream interface, or `0` if no such assert is in received.

Assert Metric Preference
The preference advertised by the assert winner on the upstream interface, or `0` if no such assert is in effect.

RPT Bit
The value (`true` or `false`) of the RPT-bit advertised by the assert winner on the upstream interface. This value is `false` if no such assert is in effect.

Route Flags
Describes PIM-specific flags related to a multicast state entry. See the PIM Sparse Mode specification for the meaning of the RPT and SPT bits.

PIM Rendezvous Point Sets Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Rendezvous Point Sets**.*

This view provides the Rendezvous Point Sets table, described below.

Rendezvous Point Sets Table

This table lists PIM information for candidate Rendezvous Points (RPs) for IP multicast groups. When the local router is the BSR, this information is obtained from received Candidate-RP-Advertisements. When the local router is not the BSR, this information is obtained from received RP-Set messages.

Component
A number uniquely identifying the component. Each protocol instance connected to a separate domain should have a different index value.

Group Address
The IP multicast group address which, when combined with **Group Mask** (Page 99), gives the

group prefix for which this entry contains information about the Candidate-RP.

Group Mask
The multicast group address mask which, when combined with **Group Address** (Page 98), gives the group prefix for which this entry contains information about the Candidate-RP.

Address
The IP address of the Candidate-RP.

Hold Time
The holdtime of a Candidate-RP. If the local router is not the BSR, this value is `0`.

Expiry Time
The minimum time remaining before the Candidate-RP will be declared down. If the local router is not the BSR, this value is `0`.

PIM IPM Route Next Hop Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **PIM IPM Route Next Hop**.*

This view provides the PIM IPM Route Next Hop table, described below.

PIM IPM Route Next Hop Table

This table lists PIM-specific information on a subset of the rows of the *IPM Route Next Hop Table* (Page 88). Each entry in the IPM Route Next Hop Table whose interface is running PIM and whose *State* (Page 89) is `pruned` has a corresponding entry in the PIM IPM Route Next Hop Table. This table contains the following information.

Group Address
Same as *Group* (Page 88) in the IPM Route Next Hop table.

Source Address
Same as *Source* (Page 88) in the IPM Route Next Hop table.

Source Mask
Same as *Source Mask* (Page 89) in the IPM Route Next Hop table.

IF Index
Same as *IF Index* (Page 89) in the IPM Route Next Hop table.

Address
Same as *Address* (Page 89) in the IPM Route Next Hop table.

Prune Reason
Indicates why the downstream interface was pruned, whether in response to a PIM prune message or due to PIM Assert processing. Possible values are `other`, `prune`, and `assert`.

PIM Candidate Rendezvous Point Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Candidate Rendezvous Point**.*

This view provides the PIM Candidate Rendezvous Point table, described below.

PIM Candidate Rendezvous Point Table

This table lists the IP multicast groups for which the local router is to advertise itself as a Candidate-RP when the value of *Hold Time* (Page 102) is non-zero. If this table is empty, then the local router will advertise itself as a Candidate-RP for all groups (providing the value of *Hold Time* is non- zero). This table contains the following information.

Group Address
The IP multicast group address which, when combined with **Group Mask** (Page 101), identifies a group prefix for which the local router will advertise itself as a Candidate-RP.

Group Mask
The multicast group address mask which, when combined with **Group Address** (Page 100), identifies a group prefix for which the local router will advertise itself as a Candidate-RP.

Address
The (unicast) address of the interface which will be advertised as a Candidate-RP.

Row Status
The status of this row, by which new entries may be created, or old entries deleted from this table. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

PIM Component Table View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Component**.*

This view provides the PIM Component table, described below.

PIM Component Table

This table contains fields specific to a PIM domain. One row exists for each domain to which the router is connected. A PIM-SM domain is defined as an area of the network over which Bootstrap messages are forwarded. Typically, a PIM-SM router will be a member of exactly one domain. This table also supports, however, routers which may form a border between two PIM-SM domains and do not forward Bootstrap messages between them. Double-clicking any entry in this table opens the PIM Component Table Entry view, which displays information for and allows configuration of that entry. This table contains the following information.

Index
A number uniquely identifying the component. Each protocol instance connected to a separate domain should have a different index value. Routers that only support membership in a single PIM-SM domain should use an **Index** value of 1.

BSR Address
The IP address of the bootstrap router (BSR) for the local PIM region.

BSR Expiry Time
The minimum time remaining before the bootstrap router in the local domain will be declared down. For candidate BSRs, this is the time until the component sends an RP-Set message. For other routers, this is the time until it may accept an RP-Set message from a lower candidate BSR.

Hold Time
The holdtime of the component when it is a candidate RP in the local domain. The value of `0` is used to indicate that the local system is not a Candidate-RP.

Status
The status of this entry. Creating the entry creates another protocol instance; destroying the entry disables a protocol instance. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Cisco PIM Objects View

Access: *From the **Icon Subviews** menu for the CiscoPIMApp Application icon, select **Cisco PIM**.*

This view contains the following Cisco-specific information for Protocol Independent Multicast (PIM) management. These fields are an extension of the values defined in the IETF PIM MIB (RFC 2934).

Invalid Register Msgs Rcvd
A count of the number of invalid PIM Register messages received by this device. A PIM Register message is termed invalid if:

- The encapsulated IP header is malformed.
- The destination of the PIM Register message is not the RP (Rendezvous Point) for the group in question.
- The source/DR (Designated Router) address is not a valid unicast address.

Invalid Join Prune Msgs Rcvd
A count of the number of invalid PIM Join/Prune messages received by this device. A PIM Join/Prune message is termed invalid if the RP specified in the packet is not the RP for the group in question.

Last Error Type
The type of the last invalid message that was received by this device. Possible values are `none`, `invalidRegister`, and `invalidJoinPrune`.

Last Error Origin Type
The type of address stored in **Last Error Origin**. This value is irrelevant if the value of **Last Error Type** is `none`. Possible values are `unknown`, `ipv4`, `ipv6`, and `dns`.

Last Error Origin
Represents the Network Layer Address of the source that originated the last invalid packet. The type of address stored depends on the value in **Error Origin Type**. This value represents the Network Layer Address of the Designated Router (DR) whenever the value of **Last Error Group** is a zero-length address, for example, when encapsulated IP header is malformed. This value is irrelevant if the value of **Last Error Type** is `none`.

Last Error Group Type
The type of address stored in **Last Error Group**. This value is `unknown` if there is a problem in the packet received from the DR. This value is irrelevant if the value of **Last Error Type** is `none`. Possible values are `unknown`, `ipv4`, `ipv6`, and `dns`.

Last Error Group
The IP multicast group address to which the last invalid packet was addressed. The type of address stored depends on the value in **Last Error Group Type**. This value is a zero-length InetAddress if there is a problem in the packet received from the DR, for example, a malformed encapsulated IP header. This value is irrelevant if the value of **Last Error Type** is `none`.

Last Error RP Type
Represents the type of address stored in **Last Error RP**. This value is irrelevant if the value of **Last Error Type** is `none`. Possible values are `unknown`, `ipv4`, `ipv6`, and `dns`.

Last Error RP
The address of the RP, as per the last invalid packet. The type of address stored depends on the value in **Last Error RP Type**. This value is irrelevant if the value of **Last Error Type** is `none`.

RP Mapping Change Type
Describes the operation that resulted in generation of a **Mapping Change** notification.

- `newMapping`, as the name suggests indicates that a new mapping has been added into the *Rendezvous Point Sets Table* (Page 98).
- `deletedMapping` indicates that a mapping has been deleted from the *Rendezvous Point Sets Table* (Page 98).
- `modifiedXXXMapping` indicates that an RP mapping (which already existed in the table) has been modified. The two modifications types, `modifiedOldMapping` and `modifiedNewMapping`, are defined to differentiate the notification generated before modification from that generated after modification.

Cisco VPDN Application

This application (CiscoVPDNApp) provides information on Virtual Private Dialup Networks (VPDNs) which handle the forwarding of PPP links from an Internet Service Provider (ISP) to a Home Gateway. It allows access to the following views:

- *Cisco VPDN System Info View*
- *Cisco VPDN Tunnel Attribute View* (Page 105)
- *Cisco VPDN Tunnel Session View* (Page 107)
- *Cisco VPDN User Failure History View* (Page 109)

Cisco VPDN System Info View

Access: *From the **Icon Subviews** menu for the CiscoVPDNApp Application icon, select **System Information.***

This view provides the System Table which contains the following information about the VPDN system for all tunnel types.

Type
The tunnel type. This is the tunnel protocol. Possible values are `12f` and `12tp`.

Tunnel Total
The total number of VPDN tunnels, of this tunnel type, that are currently active.

Session Total
The total number of active sessions, of this tunnel type, in all the active VPDN tunnels.

Denied User Total
The total number of denied user attempts to all the VPDN tunnels of this tunnel type since last system re-initialization.

Cisco VPDN Tunnel Attribute View

Access: *From the **Icon Subviews** menu for the CiscoVPDNApp Application icon, select **Tunnel Attributes.***

This view provides the Tunnel Attr Table which contains the following information about the active VPDN tunnels. An entry is added to the table when a new tunnel is initiated and removed from the table when the tunnel is terminated.

Index
A unique value identifying an entry in the table.

Local Name
The local name of an active VPDN tunnel. It will be the NAS/LAC name of the tunnel if the router serves as NAS/LAC, or the HGW/LNS name of the tunnel if the system serves as the home gateway. Typically, the local name is the configured host name of the router.

Remote Name
The remote name of an active VPDN tunnel. It will be the home gateway name of the tunnel if the system is a NAS/LAC, or the NAS/LAC name of the tunnel if the system serves as the home gateway.

Remote Endpoint Name
The remote end point name of an active VPDN tunnel. This name is either the domain name or the DNIS that this tunnel is projected with.

Local Init Conn
This object indicates whether the tunnel originated locally.

Original Cause
The cause that originated an active VPDN tunnel. The tunnel can be projected via domain name, DNIS or a stack group.

Tunnel Attr State
The current state of an active VPDN tunnel. Tunnels of type `l2f` will have states with the 'l2f' prefix. Tunnels of type `l2tp` will have states with the 'l2tp' prefix. Possible states are described in Table 12.

Table 12: Tunnel Attr States

State	Description
unknown	The current state of the tunnel is unknown.
l2fOpening	The tunnel has just been initiated and is waiting for a reply from the remote end to complete the process.
l2fOpenWait	This end received a tunnel open request from the remote end and is waiting for the tunnel to be established.
l2fOpen	The tunnel is active.
l2fClosing	This end received a tunnel close request.
l2fCloseWait	The tunnel has just been shut down and is waiting for the remote end to reply in order to complete the process.
l2tpIdle	No tunnel is initiated yet.
l2tpWaitCtlReply	The tunnel has been initiated and is waiting for a reply from the remote end to complete the process.
l2tpEstablished	The tunnel is active.
l2tpShuttingDown	The tunnel is in the process of shutting down.
l2tpNoSessionLeft	There is no session left in the tunnel.

Active Sessions
The number of active sessions currently in the tunnel.

Denied Users
The number of users denied access to the tunnel.

Soft Shut
Indicates whether a state of “soft-shutdown” has been initiated, and if so, prevents any new sessions from being added.

Network Service Type
The type of network service used in the active tunnel.

Local IP Addr
The local IP address of the tunnel. This IP address is that of the interface at the local end of the tunnel.

Source IP Addr
The Source IP address of the tunnel. This IP address is the user configurable IP address for Stack Group Biding Protocol.

Remote IP Addr
The remote IP address of the tunnel. This IP address is that of the interface at the remote end of the tunnel.

Cisco VPDN Tunnel Session View

Access: *From the **Icon Subviews** menu for the CiscoVPDNApp Application icon, select **Tunnel Sessions.***

This view contains the Session Attr Table which provides the following information about individual user sessions within the active tunnels.

Index
A unique value identifying an active user session.

User Name
The name of the user of this session.

Tunnel State
The current state of an active user session. These states are described in Table 13.

Table 13: Tunnel States

State	Description
unknown	The current state of the tunnel's session is unknown.
opening	The user session has just been initiated through a tunnel and is waiting for a reply from the the remote end to complete the process.
open	The user session is active.
closing	The user session has just been closed and is waiting for a reply from the remote end to complete the process.
waitingForTunnel	The user session is in this state when the tunnel which this session is going through is still in a closed state.

Call Duration
The call duration of the current active user session.

Packets Out
The total number of output packets through this active user session.

Bytes Out
The total number of output bytes through this active user session.

Packets In
The total number of input packets through this active user session.

Bytes In
The total number of input bytes through this active user session.

Device Type
On the local end of the tunnel, the type of physical device to which this user session is attached These types are described in Table 14.

Table 14: Device Types

Type	Description
other	Any device that has not been defined.
asyncInternalModem	Modem Pool device of an access server.
async	A regular asynchronous serial interface.
sync	A regular synchronous serial interface.
virtualAccess	Virtual Access.
bchan	An ISDN call.
xdsl	Future application with xDSL devices.
cable	Future application with Cable modem devices.

Device Caller ID
The incoming caller identification of the user. This is the originating number that called into the device that initiated the user session. This can be blank since not all devices can provide caller ID information.

Multi Link
Indicates whether the session is part of a multilink.

Note: The following entries will only contain a value for a device of type `asyncInternalModem`.

Modem Slot Index
The Modem Pool database slot index if it is associated with this user session.

Modem Port Index
The Modem Pool database port index if it is associated with this user session.

DS1 Slot Index
The DS1 database slot index if it is associated with this user session.

DS1 Port Index
The DS1 database port index if it is associated with this user session.

DS1 Chan Index
The DS1 database channel index if it is associated with this user session.

Call Start Time
The start time of the current modem call.

Call Start Index
Arbitrary small integer to distinguish modem calls that occurred at the same time tick.

Cisco VPDN User Failure History View

Access: *From the **Icon Subviews** menu for the CiscoVPDNApp Application icon, select **User Failure History.***

This view provides the User Failure History table, which is a record of failure entries that can be referenced by a user name. Only a name that has a valid item in the Cisco IOS VPDN failure history table will yield a valid entry in this table. The User Failure History table keeps up to a maximum of 50 of the newest entries only and displays the following information.

Index
A unique value used to identify an entry in the table.

User Name
The user name for this entry.

Tunnel ID
The Tunnel ID for this entry. If it is the initiator of the tunnel, the ID is the HGW/LNS tunnel ID, otherwise it is the NAS/LAC tunnel ID.

User ID
The user ID of this entry.

Local Init Conn
Indicates whether the tunnel in which the failure occurred was generated locally or not.

Local Name
The local name of the VPDN tunnel in which the failure occurred. It will be the NAS/LAC name of the tunnel if the router serves as a NAS/LAC, or the HGW/LNS name of the tunnel if the system serves as the home gateway. The local name is the configured host name of the router.

Remote Name
The remote name of the VPDN tunnel in which the failure occurred. It will be the home gateway name of the tunnel if the system is a NAS/LAC, or the NAS/LAC name of the tunnel if the system serves as the home gateway. This object can be empty if the failure occurred prior to successful tunnel projection, thus no source name will be available.

Source IP
The source IP address of the tunnel in which the failure occurred. This IP address is the interface at the initiator end of the tunnel.

Dest IP
The destination IP address of the tunnel in which the failure occurred. This IP address is the interface at the receiver end of the tunnel.

Hist Count
Number of multiple failures that have been experienced by this user on this tunnel. Seeing a delta of >1 is an indication that the current failure record is the latest in a series of failures.

Fail Time
The time the failure occurred.

Fail Type
The type of failure for the entry.

Fail Reason
The reason for the failure.

Cisco DLSW Ext Application

This application (CiscoDLSWExtApp) supports the CISCO-DLSW-EXT-MIB. This is the MIB module for management of Cisco-specific Data Link Switching protocol enhancements. This application provides access to the following views:

- *Cisco DLSW Ext Node View*
- *Cisco DLSW Ext Transport Connection Config View* (Page 116)
- *Cisco DLSW Ext Transport Connection Operation View* (Page 119)
- *Cisco DLSW Ext Transport Connection Specific View* (Page 121)
- *Cisco DLSW Ext Transport Connection Direct Config View* (Page 121)
- *Cisco DLSW Ext Interface View* (Page 122)
- *Cisco DLSW Ext Fast View* (Page 123)
- *Cisco DLSW Ext Circuit View* (Page 124)
- *Cisco DLSW Ext Trap Control View* (Page 125)

Cisco DLSW Ext Node View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Node.***

This view provides the following information.

T Addr
The local peer IP address. This is required for Fast-Sequenced Transport (FST) and TCP. If no local peer IP address is configured then this value will be the empty string.

Group
Peer group number for this router. Peer groups are arbitrary groups of routers with one or more designated border peers. Border peers form peer connections with every router in their group and with border peers in other groups. The role of a border peer is to forward explorers on behalf of other routers. A value of zero means no group has been set and the DLSw is not a group member.

Border
This variable indicates if this DLSw is capable of operating as a border peer. `True` indicates that it is capable, `false` indicates that it is not. Border peers form peer connections with every router in their group and with border peers in other groups. The role of a border peer is to forward explorers on behalf of other DLSw routers. The default value is `false`.

Cost
Peer cost advertised to remote peers in the capabilities exchange. If an end station can be reached through more than one peer, the cost of each peer will be considered when a circuit is established. A lower cost indicates that peer will be the preferred choice if there is more than one path to the destination. A value of zero means no cost has been set and that cost will not be considered during circuit establishment.

Keep Alive Interval
Default remote peer keepalive interval in seconds. The keepalive parameter refers to how often DLSw peers send peer keep alives to each other. These periodic messages allow DLSw to keep track of the state of all peers. If set to zero, no keepalives are sent.

Passive Connect
This variable indicates if DLSw will not initiate remote peer connections to configured peers. True indicates that it will not initiate remote peer connections, false indicates that it will initiate remote peer connections. In other words a passive peer will wait for the remote peer to initiate a peer connection. The default value is `false`.

BIU Segment
This variable indicates if DLSw will spoof the maximum receivable Basic Information Unit (frame) size in XID so that each end station sends the largest frame it can. True indicates that it will spoof, false indicates that it will not. The default value is `false`.

Init Pacing Window
Initial pacing window size. This is the starting size of the pacing window. DLSw uses an adaptive pacing flow control algorithm that automatically adjusts to congestion levels in the network. Pacing windows are used to control how many packets may be sent to a peer before acknowledgement.

Max Pacing Window
Maximum pacing window size. This is the largest size that the pacing window will grow to. DLSw uses an adaptive pacing flow control algorithm that automatically adjusts to congestion levels in the network. Pacing windows are used to control how many packets may be sent to a peer before acknowledgement.

Promiscuous
This variable indicates if DLSw will accept connections from non-configured remote peers. Promiscuous routers will accept peer connection requests from routers that are not preconfigured. This feature allows central site routers to remain unchanged when branch offices are added or deleted. It also minimizes required coordination of

configurations. True indicates that it will accept connections, false indicates that it will not. The default value is `false`.

Peer Default Cost

This variable indicates the cost that will be used with promiscuous peers. If an end station can be reached through more than one peer, the cost of each peer will be considered when a circuit is established. A lower cost indicates that peer will be the preferred choice if there is more than one path to the destination.

Peer Dest MAC

Permits the promiscuous peer connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address. If no default destination mac is configured then this object will be the empty string.

Peer Keep Alive Int

Default promiscuous peer keepalive interval in seconds. The keepalive parameter refers to how often DLSw peers send peer keep alives to each other. These periodic messages allow DLSw to keep track of the state of all peers. If set to zero, no keepalives are sent.

Peer LF Size

The default Largest Frame Size associated with the default promiscuous peer transport connection. In other words it's the largest size of the INFO field (including DLC header, not including any MAC-level or framing octets). Possible values appear in Table 15 (Page 113).

Table 15: Peer LF Size Values

Value	Largest Frame Size
lfs516	516
lfs635	635
lfs754	754
lfs873	873
lfs993	993
lfs1112	1112
lfs1231	1231
lfs1350	1350
lfs1470	1470
lfs1542	1542
lfs1615	1615
lfs1688	1688
lfs1761	1761
lfs1833	1833
lfs1906	1906
lfs1979	1979

Table 15: Peer LF Size Values (Continued)

Value	Largest Frame Size
lfs2052	2052
lfs2345	2345
lfs2638	2638
lfs2932	2932
lfs3225	3225
lfs3518	3518
lfs3812	3812
lfs4105	4105
lfs4399	4399
lfs4865	4865
lfs5331	5331
lfs5798	5798
lfs6264	6264
lfs6730	6730
lfs7197	7197
lfs7663	7663
lfs8130	8130
lfs8539	8539
lfs8949	8949

Table 15: Peer LF Size Values (Continued)

Value	Largest Frame Size
lfs9358	9358
lfs9768	9768
lfs10178	10178
lfs10587	10587
lfs10997	10997
lfs11407	11407
lfs12199	12199
lfs12992	12992
lfs13785	13785
lfs14578	14578
lfs15370	15370
lfs16163	16163
lfs16956	16956
lfs17749	17749
lfs20730	20730
lfs23711	23711
lfs26693	26693
lfs29674	29674
lfs32655	32655

Table 15: Peer LF Size Values (Continued)

Value	Largest Frame Size
lfs38618	38618
lfs41600	41600
lfs44591	44591
lfs47583	47583
lfs50575	50575
lfs53567	53567
lfs56559	56559
lfs59551	59551
lfs65535	65535

Peer TCP Queue Max
Default promiscuous peer maximum output TCP queue size. For DLSw over TCP encapsulation, packets may be queued due to congestion of the TCP network. This variable is used to set the output queue maximum of the underlying TCP connection, by default on a promiscuous peer transport connection.

On Demand Cost
This variable indicates the cost that will be used with peer on demand peers. If an end station can be reached through more than one peer, the cost of each peer will be considered when a circuit is established. A lower cost indicates that peer will be the preferred choice if there is more than one path to the destination.

On Demand FST
This variable indicates if Fast-Sequenced Transport (FST) will be for peer on demand peers. True indicates that FST will be used, false indicates that it will not. The default value is `false`.

On Demand Inactivity Int
This variable indicates the length of time a peer on demand connection can be idle before shutting down this peer on demand connection. If set to zero, the peer on demand connection will not be closed due to inactivity.

On Demand Keep Alive Int
Default peer on demand keepalive interval in seconds. The keepalive parameter refers to how often DLSw peers send peer keep alives to each other. These periodic messages allow DLSw to keep track of the state of all peers. If set to zero, no keepalives are sent.

On Demand LF Size
The default Largest Frame Size associated with the default peer on demand transport connections. In other words, it's the largest size of the INFO field (including DLC header, not including any MAC-level or framing octets). Possible values appear in Table 15 (Page 113).

On Demand Priority
This variable indicates if circuit prioritization will be used for peer-on-demand peers. True indicates that circuit prioritization specified by the dlswCircuitPriority object in the DLSW-MIB (RFC 2024) will be used, false indicates that there will be no circuit prioritization. The default value is `false`.

On Demand TCP Queue Max
Default peer-on-demand Maximum output TCP queue size. For DLSw over TCP encapsulation, packets may be queued due to congestion of the TCP network. This variable is used to set the output queue maximum of the underlying TCP connection, by default on a peer on demand transport connection.

Cisco DLSW Ext Transport Connection Config View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Transport Connections > Configuration.***

This view provides the **cde TConn Config Table**. This table defines the peer transport connections that will be initiated or accepted by this DLSw. Structure of masks allows wildcard definition for a collection of transport connections by a conceptual row. For a specific transport connection, there may be multiple conceptual rows that match the transport address. The "best" match will be the one to determine the characteristics of the transport connection. Double-clicking an entry in this table opens a Table Entry view which lets you configure that entry. The cde TConn Config Table augments **dlswTConnConfigTable** and contains the following information.

Index
The unique identifier for this entry.

T Domain
The type of DLSw encapsulation in use on this peer connection. Possible values are `tcp`, `fst`, `directHdlc`, `directFrameRelay`, and `llc2`. The default value is `tcp`.

Local Ack
Reflects whether the peer connection is locally acknowledged. Local acknowledgement means terminating the DLC connections at the router, eliminating the requirement for link-layer acknowledgements and keepalive messages to flow across the WAN. In addition, because link-layer frames are acknowledged locally, link-layer time-outs should not occur. In general, **ciscoDlswTConnConfigLocalAck** will be true when *T Domain* (Page 116) is `tcp`, false when it is `fst`, `direct-Hdlc`, or `directFrameRelay`. When the remote-peer is configured as pass-thru, it will not use local acknowledgement. The default value is `true`.

Cost
The cost associated with the transport connection, assigned to this conceptual row representing a peer. If an end station can be reached through more than one peer, the cost of each peer will be considered when a circuit is established. A lower cost indicates that peer will be the preferred choice if there is more than one path to the destination.

LF Size
The Largest Frame Size associated with the transport connection. This is the largest size of the INFO field (including DLC header, not including any MAC-level or framing octets). Possible values appear in Table 15 (Page 113).

Keep Alive Int
The amount of time between keepalive messages on a transport connection. The keepalive parameter refers to how often DLSw peers send peer keep alives to each other. These periodic messages allow DLSw to keep track of the state of all peers. If set to zero, no keepalives are sent.

Backup
This variable indicates if this peer is defined as a backup to an existing peer. A backup peer is used to provide an alternate path in case an existing peer becomes unavailable. A backup peer will not enter the connected state until the primary peer that it backs up becomes disconnected. True indicates that this conceptual row is a backup peer to a pre-existing peer, false indicates this peer is not a backup peer. The default value is `false`.

Backup T Addr
The primary peer's IP address that this entry backs up. Valid only when **ciscoDlswTConnConfigBackup** is `true`.

Backup Linger
This variable indicates whether the backup peer will remain connected after the primary peer connection has been re-established. True indicates that the backup peer will remain connected after the primary peer connection has been re-established, for the length of time specified in *Backup Linger Int*. False indicates that the backup peer will remain connected until all circuits on the backup peer connection have been disconnected. The default value is `false`.

Backup Linger Int
This variable indicates the length of time the backup peer remains connected after the primary peer connection has been re-established. If this variable is zero, the backup peer will be disconnected immediately after the primary peer connection has been re-established. If greater than zero the backup will stay connected for the number of minutes indicated by this variable, after the primary peer connection has been re-established. Note that the linger interval is only used when *Backup Linger* is true.

Priority
Indicator of whether this peer connection supports priority. When priority is configured for the remote peer, DLSw+ will automatically activate four TCP connections to that remote peer (ports 2065, 1981, 1982, and 1983). Priority only needs to be configured if you need to prioritize between SNA and NetBIOS, or within SNA by LOCADDR or MAC/SAP pair (known as SAP prioritization). In addition, this granular packet classification is only possible when TCP encapsulation is selected for a specific remote peer. By default DLSw+ assigns certain traffic to specific TCP ports. The default value is `false`.

Dest MAC
Permits the peer connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address. If no explorer traffic with a destination address of **Dest MAC** is received by DLSw, the peer represented by this conceptual row will not be connected.

Dynamic
Indicates the peer connection is to be established only when there is DLSw+ data to send. The default value is `false`.

Dynamic No LLC
This variable indicates the length of time a dynamic peer remains connected after all LLC2 circuits are gone.

Dyn Inactivity Interval
Indicates the length of time a connection can be idle before closing the dynamic peer connection. If set to zero, the dynamic peer connection will not be closed due to inactivity.

Cisco DLSW Ext Transport Connection Operation View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Transport Connections > Operation.***

This view provides the **cde TConn Oper Table**. This table is a list of peer transport connections. Each connected peer will create a conceptual row in the table. When the peer disconnects, the row will be deleted from the table. This table augments **dlswTConnOperTable** and contains the following information.

Index
A unique value identifying an entry in the table.

Cost
The partner's cost on this peer connection, as received through capabilities exchange. If an end station can be reached through more than one peer, the cost of each peer will be considered when a circuit is established. A lower cost indicates that peer will be the preferred choice if there is more than one path to the destination.

Priority
The partner's priority setting on this peer connection, as received through capabilities exchange. When priority is enabled for the remote peer, DLSw+ will automatically activate four TCP connections to that remote peer (ports 2065, 1981, 1982, and 1983). Priority only needs to be configured if you need to prioritize between SNA and NetBIOS, or within SNA by LOCADDR or MAC/SAP pair (known as SAP prioritization). In addition, this granular packet classification is only possible when TCP encapsulation is selected for a specific remote peer. By default DLSw+ assigns certain traffic to specific TCP ports.

Border Peer
This variable indicates if the partner DLSw is capable of operating as a border peer, as received through capabilities exchange. True indicates that it is capable, false indicates that it is not. Border peers form peer connections with every router in their group and with border peers in other groups. The role of a border peer is to forward explorers on behalf of other DLSw routers.

Group Num
This variable indicates the partner's group number, as received through capabilities exchange. Peer groups are arbitrary groups of routers with one or more designated border peers. Border peers form peer connections with every router in their group and with border peers in other groups. The role of a border peer is to forward explorers on behalf of other routers. A value of zero means no group has been set and the DLSw is not a group member.

Domain Type
The type of DLSw encapsulation in use on this peer connection. Possible values are `tcp`, `fst`, `directHdlc`, `directFrameRelay`, and `llc2`.

Cisco DLSW Ext Transport Connection Specific View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Transport Connections > Specific.***

This view provides the **cde TConn Tcp Config Table**. This table defines the TCP transport connections that will be either initiated by or accepted by this DSLw. It augments the entries in dlswTConnConfigTable whose domain is dlswTCPDomain. In other words, for each conceptual row in the dlswTConnConfigTable, if the dlswTConnConfigTDomain is dlswTCPDomain, that conceptual row will be augmented by this table. dlswTCPDomain, dlswTConnConfigTable, and dlswTConnConfigTDomain are all imported from DLSW-MIB (RFC 2024). This table augments dlswTConnTcpConfigTable and contains the following information.

Index
The index to the conceptual row of the table, derived from dlswTConnConfigIndex.

Queue Max
Maximum output TCP queue size for this remote peer. For DLSw over TCP encapsulation, packets may be queued due to congestion of the TCP network. This variable is used to set the output queue maximum of the underlying TCP connection for the peer represented by the conceptual row.

Cisco DLSW Ext Transport Connection Direct Config View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Transport Connections > Direct Configuration.***

This view provides the **cde TConn Direct Config Table**. This table contains direct peer media-specific configuration information. An entry is maintained for every peer in the **cdeTConnConfigTable** (Page 116) whose domain is either cdeDirectHdlcDomain, cdeDirectFrameRelayDomain, or cdeLlc2Domain. In other words, for each conceptual row in the dlswTConnConfigTable, if the dlswTConnConfigTDomain is either cdeDirectHdlcDomain, cdeDirectFrameRelayDomain, or cdeLlc2Domain, there will be an entry in this table.

dlswTConnConfigTable and **dlswTConnConfigTDomain** are imported from DLSW-MIB (RFC 2024). This table contains the following information.

Index
The index to the conceptual row of the table, derived from **dlswTConnConfigIndex**.

If Index
The IfEntry index of the local interface, on which the direct peer can be reached.

Media Encap
The type of media encapsulation to be used on this peer connection. When using DLSw Direct-encapsulation or DLSw Lite (Frame Relay) encapsulation, the peer transport connection is defined as either directHdlc or directFrameRelay, respectively. Hdlc peer transport encapsulation does not support local acknowledgment of frames. Logical Link Control, Type2 (LLC2) peer transport encapsulation -for transport across a point-to-point connection (currently only Frame Relay is supported) provides local acknowledgment and reliable transport. Possible values are `directHdlc`, `directFrameRelay`, and `llc2`. The default value is `directHdlc`.

Relay DLCI
The Data Link Connection Identifier for the virtual circuit on this interface. This field will only be valid if the value of *Media Encap* (Page 122) is `llc2`.

Cisco DLSW Ext Interface View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Interface***

This view provides the **cde If Table**. This table lists the interfaces on which DLSw is active. The cde If Table augments the **dlswIfTable**.

Index
The interface index for this entry.

If Type
The DLC protocol in use on this DLSw interface. Possible values are `other`, `na`, `llc`, `sdlc`, and `qllc`.

Cisco DLSW Ext Fast View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Interface***

This view provides the **cde Fast Table**, a table containing fast cache entries. The table contains cache information for FST peers or direct encapsulation peers (without local acknowledgement enabled). When using these encapsulation types, a fast-switching cache must be built. The first frame between two end stations will be process switched, and during this process an entry will be made in the fast-switching cache so that subsequent frames between those end stations may be fast switched. End station 1 (S1) and End station 2 (S2) are used to represent the two end stations of the fast cache entry. S1 is always an end station which is locally attached. S2 is always an end station which is remote. This table contains the following information.

Index
A unique value identifying an entry in the table.

If Index
The ifEntry index of the local interface through which S1 can be reached.

S1 Route Info
If source-route bridging is in use between the DLSw and S1, this is the routing information field describing the path between the two devices. Otherwise the value will be an OCTET STRING of zero length.

S1 Cache ID
The Cache ID assigned by this DLSw to this fast cache entry. Every Fast cache entry will have a unique id. A management station could use this value by periodically polling this table, and determine whether the same cache entries were present or absent.

S2 T Domain
This field contains the transport domain of the peer transport protocol that the fast cache entry is running over.

S2 T Address
The transport address of the partner DLSw

S2 Cache ID
The Cache ID assigned to this fast cache entry by the partner DLSw. Every Fast cache entry will have a unique id. A management station could use this value by periodically polling this table, and determine whether the same cache entries were present or absent.

Origin
Specifies which of the two end stations initiated the establishment of this circuit. Possible values are `s1` and `s2`.

Time To Live
The amount of time (in hundredths of a second) remaining before this fast cache entry will be removed from the table. After 5 minutes of inactivity, the fast cache entry will be deleted.

Cisco DLSW Ext Circuit View

Access: *From the **Icon Subviews** menu for the CiscoDLSWExtApp Application icon, select **Circuit***

This view provides the **cde Circuit Table**, which is a list of circuits. Each new circuit will create a conceptual row in the table. When the circuit disconnects, the row will be deleted from the table. End station 1 (S1) and End station 2 (S2) are used to represent the two end stations of the circuit. S1 is always an end station which is locally attached. S2 may be locally attached or remote. This table augments the **dlswCircuitTable** and contains the following information.

Index
A unique value identifying an entry in the table.

S1 Name
Represents the PU Name of End Station 1 (S1), if available.

S2 Name
Represents the PU Name of End Station 2 (S2), if available.

S1 Id Block
The block number is the first three digits of the SNA Node id of End Station 1 (S1), if available. These 3 hexadecimal digits identify the product.

S1 Id Num
The ID number is the last 5 digits of the SNA Node id of End Station 1 (S1), if available. These 5 hexadecimal digits are administratively defined and combined with the 3 digit block number form the Node id. This Node id is used to identify the local node and is included in SNA XIDs.

Cisco DLSW Ext Trap Control View

Access: *From the* ***Icon Subviews*** *menu for the CiscoDLSWExtApp Application icon, select* ***Trap Control***

This view provides the following information.

T Conn

Indicates whether DLSw is permitted to emit transport connection up and down traps. With the value of `true`, DLSw will emit traps when connections enter `connected` and `disconnected` states. With the value of `false`, DLSw will not emit traps when connections enter `connected` and `disconnected` states. The changes take effect immediately. The default value is `false`.

Circuit

Indicates whether the DLSw is permitted to generate circuit up and down traps. With the value of `true` the DLSw will emit traps when circuits enter `connected` and `disconnected` states. With the value of `false`, the DLSw will not emit traps when circuits enter `connected` and `disconnected` states. The changes take effect immediately.

Cisco DLSW Application

This application (**CiscoDLSWApp**) supports the CISCO-DLSW-MIB. This MIB module lets you manage Data Link Switches. This application provides access to the following views:

- *Cisco DLSW Node View* (Page 126)
- *Cisco DLSW Transport Connection Statistics View* (Page 129)
- *Cisco DLSW Transport Connection Config View* (Page 129)
- *Cisco DLSW Transport Connection Operation View* (Page 132)
- *Cisco DLSW Transport Connection TCP Config View* (Page 137)
- *Cisco DLSW Transport Connection TCP Operation View* (Page 138)
- *Cisco DLSW Interface View* (Page 138)
- *Cisco DLSW Dir MAC Cache View* (Page 139)
- *Cisco DLSW Dir NBIOS Cache View* (Page 141)
- *Cisco DLSW Dir Location View* (Page 143)
- *Cisco DLSW Circuit View* (Page 143)
- *Cisco DLSW SDLC View* (Page 148)

Cisco DLSW Node View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Node.***

This view provides the following information.

Version

This value identifies the particular version of the DLSw standard supported by this DLSw. The first octet is a hexadecimal value representing the DLSw standard Version number of this DLSw, and the second is a hexadecimal value representing the DLSw standard Release number. This information is reported in DLSw Capabilities Exchange.

Version String

This string gives product-specific information about this DLSw (e.g., product name, code release and fix level). This flows in Capabilities Exchange messages.

Vendor ID

The value identifies the manufacturer's IEEE-assigned organizationally Unique Identifier (OUI) of this DLSw. This information is reported in DLSw Capabilities Exchange.

Std Pacing Support

Circuit pacing, as defined in the DLSw Standard, allows each of the two DLSw nodes on a circuit to control the amount of data the other is permitted to send to them. This value reflects the level of support an implementation has for this protocol, as listed in Table 16.

Table 16: DLSw Standard Pacing Support

Value	Meaning
`none`	The node has no support for the standard circuit pacing flows; it may use RFC 1434+ methods only, or a proprietary flow control scheme.
`adaptiveRcvWindow`	The node supports the standard scheme and can vary the window sizes it grants as a data receiver.
`fixedRcvWindow`	The node supports the standard scheme but never varies its receive window size.

Status
The status of the DLSw part of the system.

Since the following are destructive actions, the user should query the circuit and transport connection tables in advance to understand the effect this action will have.

Changing the value from `active` to `inactive` causes DLSw to take the following actions: (1), it disconnects all circuits through all DLSw partners, (2), it disconnects all transport connections to all DLSw partners, (3), it disconnects all local DLC connections, and, (4), it stops processing all DLC connection set-up traffic.

Changing the value from `inactive` to `active` causes DLSw to come up in its initial state, i.e., transport connections established and ready to bring up circuits.

Up Time
The time (in hundredths of a second) since the DLSw portion of the system was last re-initialized. That is, if **ciscoDlswstate** is in the active state, the time the **ciscoDlswState** entered the active state. It will remain zero if **ciscoDlswState** is in the inactive state.

Virtual Segment LF Size
The largest frame size (including DLC header and info field but not any MAC-level or framing octets) this DLSw can forward on any path through itself. This object can represent any box-level frame size forwarding restriction (e.g., from the use of fixed-size buffers). Some DLSw implementations will have no such restriction.This value will affect the LF size of circuits during circuit creation. The LF size of an existing circuit can be found in the RIF (Routing Information Field). Possible values appear in Table 15 (Page 113).

Resource NB Exclusivity
A value of `true` indicates that the NetBIOS Names configured in *Dlsw Dir NBIOS Table* (Page 141) are the only ones accessible via this DLSw. If a node supports sending run-time capabilities exchange messages, changes to this value should cause that action. It is up to the implementation exactly when to start the run-time capabilities exchange.

Resource Mac Exclusivity
A value of `true` indicates that the MAC addresses configured in the *Dlsw Dir MAC Table* (Page 139) are the only ones accessible via this DLSw. If a node supports sending run-time capabilities exchange messages, changes to this value should cause that action. It is up to the implementation exactly when to start the run-time capabilities exchange.

Partner Reject

Indicates whether the DLSw is permitted to emit partner reject related traps. With the value of `enabled` the DLSw will emit all partner reject related traps. With the value of `disabled` the DLSw will not emit any partner reject related traps. With the value of `partial` the DLSw will only emits partner reject traps for CapEx reject. The changes take effect immediately. Possible values are `enabled`, `disabled`, and `partial`.

Prot Violation

Indicates whether the DLSw is permitted to generate protocol-violation traps on the events such as window size violation. The changes take effect immediately.

Connection

Indicates whether the DLSw is permitted to emit transport connection up and down traps. With the value of `enabled`, the DLSw will emit traps when connections enter `connected` and `disconnected` states. With the value of `disabled`, the DLSw will not emit traps when connections enter `connected` and `disconnected` states. With the value of `partial` the DLSw will only emit transport connection down traps when the connection is closed with busy. The changes take effect immediately. Possible values are `enabled`, `disabled`, and `partial`.

Circuit

Indicates whether the DLSw is permitted to generate circuit up and down traps. With the value of `enabled`, the DLSw will emit traps when circuits enter `connected` and `disconnected` states. With the value of `disabled`, the DLSw will not emit traps when circuits enter `connected` and `disconnected` states. With the value of `partial` the DLSw will emit traps only for those circuits that are initiated by this DLSw, e.g., originating the CUR_CS message. The changes take effect immediately. Possible values are `enabled`, `disabled`, and `partial`.

Cisco DLSW Transport Connection Statistics View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Transport Connections > Statistics.***

This view provides the following information.

Active Connections
The number of transport connections that are not in `disconnected` state.

Close Idles
The number of times transport connections in this node exited the connected state with zero active circuits on the transport connection.

Close Busys
The number of times transport connections in this node exited the connected state with some non-zero number of active circuits on the transport connection. Normally this means the transport connection failed unexpectedly.

Cisco DLSW Transport Connection Config View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Transport Connections > Configuration**.*

This view provides the **DLSW TConn Config Table**. This table defines the transport connections that will be initiated or accepted by this DLSw. Structure of masks allows wildcard definition for a collection of transport connections by a conceptual row. For a specific transport connection there may be many conceptual rows which match the transport address. The “best” match will the one to determine the characteristics of the transport connection. The table contains the following information.

Index
The index to the conceptual row of the table.

T Domain
The object identifier which indicates the transport domain of this conceptual row.

Local T Addr
The local transport address for this conceptual row of the transport connection definition.

Remote T Addr
The remote transport address. Together with the **ciscoDlswTConnConfigRemoteTAddrMask**, the object instance of this conceptual row identifies a collection of the transport connections that will be either initiated by this DLSw or initiated by partner DLSw and accepted by this DLSw.

Last Modify Time
The value of **ciscoDlswUpTime** when the value of any object in this conceptual row was last changed. This value may be compared to **ciscoDlswTConnOperConnectTime** to determine whether values in this row are completely valid for a transport connection created using this row definition.

Entry Type
Possible values are `individual`, `global`, and `group`. The object instance signifies the type of entry in the associated conceptual row. The value of `individual` means that the entry applies to a specific partner DLSw node as identified by *Remote T Addr* and *T Domain* (Page 129). The value of `global` means that the entry applies to all partner DLSw nodes of the TDomain. The value of `group` means that the entry applies to a specific set of DLSw nodes in the TDomain. Any group definitions are enterprise-specific and are pointed to by *Group Def* (Page 130). In the cases of `global` and `group`, the value in *Remote T Addr* may not have any significance.

Group Def
For conceptual rows of `individual` and `global` as specified in *Entry Type* (Page 130), the instance of this object is `0.0`. For conceptual rows of `group`, the instance points to the specific group definition.

Setup Type
This value of the instance of a conceptual row identifies the behavior of the collection of transport connections that this conceptual row defines. The values of `activePersistent`, `activeOnDemand` and `passive` mean this DLSw will accept any transport connections, initiated by partner DLSw nodes, which are defined by this conceptual row. The value of `activePersistent` also means this DLSw will also initiate the transport connections of this conceptual row and retry periodically if necessary. The value of `activeOnDemand` also means this DLSw will initiate a transport connection of this conceptual row, if there is a directory cache hits. The value of `other` is implementation specific. The value of `exclude` means that the specified node is not allowed to be a partner to this DLSw node. To take a certain conceptual row definition out of service, a value of `notInService` for *Row Status* (Page 132) should be used. Possible values are

other, activePersistent, activeOnDemand, passive, and excluded.

Sap List

The SAP list indicates which SAPs are advertised to the transport connection defined by the local peer whose transport address is given by *Local T Addr* (Page 129). The SAP list is configured on the local peer, and the SAP list is sent to other peers via capabilities exchange. The SAP list represents the SAPs specified via the configuration command: `dlsw icanreach saps X` or `dlsw icannotreach saps X` Where `X` is in the range 0-FE.

Only SAPs with even numbers are represented, in the form of the most significant bit of the first octet representing the SAP 0, the next most significant bit representing the SAP 2, to the least significant bit of the last octet representing the SAP 254. Data link switching is allowed for those SAPs which have one in its corresponding bit, not allowed otherwise. The whole SAP list has to be changed together. Changing the SAP list affects only new circuit establishments and has no effect on established circuits.

This list can be used to restrict specific partners from knowing about all the SAPs used by DLSw on all its interfaces (these are represented in **ciscoDlswIfSapList** for each interface). For instance, one may want to run NetBIOS with some partners but not others.

If a node supports sending run-time capabilities exchange messages, changes to this value should cause that action. It is up to the implementation exactly when to start the run-time capabilities exchange. The default value of `'ffffffffffffffffffffffffffffffff'h` indicates support for all SAPs.

Advertise Mac

The value of `true` indicates that defined local MAC addresses and NetBIOS names will be advertised to a partner node via initial and (if supported) run-time capabilities exchange messages.

NB Init Cir Recv

The initial circuit receive pacing window size, in the unit of SSP messages, to be used for future transport connections activated using this table row. The managed node sends this value as its initial receive pacing window in its initial capabilities exchange message. Changing this value does not affect the initial circuit receive pacing window size of currently active transport connections. If the standard window pacing scheme is not supported, the value is zero.

A larger receive window value may be appropriate for partners that are reachable only via physical paths that have longer network delays.

Opens
Number of times transport connections entered connected state according to the definition of this conceptual row.

Row Status
Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`. This value is used by a Management Station to create or delete the row entry in the **ciscoDlswTConnConfigTable** following the RowStatus textual convention. The value of `notInService` will be used to take a conceptual row definition out of use.

Cisco DLSW Transport Connection Operation View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Transport Connections > Operation**.*

This view provides the **Dlsw TConn Operation Table** which is a list of transport connections. It contains the following information.

Index
Identifier for this row.

Local T Addr
The local transport address for this transport connection. This value could be different from **ciscoDlswTConnConfigLocalAddr**, if the value of the latter were changed after this transport connection was established.

Entry Time
The value of **ciscoDlswUpTime** when this transport connection conceptual row was created.

Connect Time
The value of ciscoDlswUpTime when this transport connection last entered the `connected` state. A value of zero means this transport connection has never been established.

State
The state of this transport connection. The transport connection enters `connecting` state when DLSw makes a connection request to the transport layer. Once initial Capabilities Exchange is sent, the transport connection enters enters `initCapExchange` state. When partner capabilities have been determined and the transport connection is ready for sending CanUReach (CUR) messages, it moves to the `connected` state. When DLSw is in the process of bringing down the connection, it is in the `disconnecting` state. When the transport layer indicates one of its connections is disconnected, the transport connection moves to the `disconnected` state.

Whereas all of the values will be returned in response to a management protocol retrieval operation, only two values may be specified in a management protocol set operation: `quiescing` and `disconnecting`. Changing the value to `quiescing` prevents new circuits from being established, and will cause a transport disconnect when the last circuit on the connection goes away. Changing the value to `disconnecting` will force off all circuits immediately and bring the connection to `disconnected` state.

Config Ind
The value of **ciscoDlswTConnConfigIndex** of the **ciscoDlswTConnConfigEntry** that governs the configuration information used by this Dlsw TConn Operation Table entry. This value is zero if the corresponding **ciscoDlswTConnConfigEntry** was deleted after the creation of this Dlsw TConn Operation Table entry. If fields in the former were changed but the conceptual row was not deleted, some configuration information may not be valid for this operational transport connection.

Flow Cntl Mode
The flow control mechanism in use on this transport connection. This value is `undetermined` before the mode of flow control can be established on a new transport connection (i.e., after CapEx is sent but before Capex or other SSP control messages have been received). A value of `pacing` indicates that the standard RFC 1795 pacing mechanism is in use. A value of `other` may be either the RFC 1434+ xBusy mechanism operating to a back-level DLSw, or a vendor-specific flow control method. Whether it is xBusy or not can be inferred from *Partner Version*.

Partner Version
This value identifies which version (first octet) and release (second octet) of the DLSw standard is supported by this partner DLSw. This information is obtained from a DLSw capabilities exchange

message received from the partner DLSw. A string of zero length is returned before a Capabilities Exchange message is received, or if one is never received. A conceptual row with a *State* (Page 133) of `connected` but a zero length partner version indicates that the partner is a non-standard DLSw partner.

Partner Vendor ID
This value identifies the IEEE-assigned organizationally Unique Identifier (OUI) of the maker of this partner DLSw. This information is obtained from a DLSw capabilities exchange message received from the partner DLSw. A string of zero length is returned before a Capabilities Exchange message is received, or if one is never received.

Partner Version Str
This value identifies the particular product version (e.g., product name, code level, fix level) of this partner DLSw. The format of the actual version string is vendor-specific. This information is obtained from a DLSw capabilities exchange message received from the partner DLSw. A string of zero length is returned before a Capabilities Exchange message is received, if one is never received, or if one is received but it does not contain a version string.

Partner Init Pacing
The value of the partner initial receive pacing window. This is our initial send pacing window for all new circuits on this transport connection, as modified and granted by the first flow control indication the partner sends on each circuit. This information is obtained from a DLSw capabilities exchange message received from the partner DLSw. A value of zero is returned before a Capabilities Exchange message is received, or if one is never received.

Partner Sap List
The Supported SAP List received in the capabilities exchange message from the partner DLSw. This list has the same format described for *Sap List* (Page 131). A string of zero length is returned before a Capabilities Exchange message is received, or if one is never received.

Partner NB Excl
The value of `true` signifies that the NetBIOS names received from this partner in the NetBIOS name list in its capabilities exchange message are the only NetBIOS names reachable by that partner. The value of `false` indicates that other NetBIOS names may be reachable. `False` should be returned before a Capabilities Exchange message is received, if one is never received, or if one is received without a NB Name Exclusivity CV.

Partner Mac Excl
The value of `true` signifies that the MAC addresses received from this partner in the MAC address list in its capabilities exchange message are the only MAC addresses reachable by that partner. The value of `false` indicates that other MAC addresses may be reachable. `False` should be returned before a Capabilities Exchange message is received, if one is never received, or if one is received without a MAC Address Exclusivity CV.

Partner NB Info
It is up to this DSLw whether to keep either none, some, or all of the NetBIOS name list that was received in the capabilities exchange message sent by this partner DLSw. This object identifies how much information was kept by this DLSw. These names are stored as userConfigured remote entries in **ciscoDlswDirNBTable**. A value of `notApplicable`, should be returned before a Capabilities Exchange message is received, or if one is never received. Possible values are `none`, `partial`, `complete`, and `notApplicable`.

Partner Mac Info
It is up to this DSLw whether to keep either none, some, or all of the MAC address list that was received in the capabilities exchange message sent by this partner DLSw. This object identifies how much information was kept by this DLSw. These names are stored as userConfigured remote entries in *Dlsw Dir MAC Table* (Page 139). A value of `notApplicable`, should be returned before a Capabilities Exchange message is received, or if one is never received. Possible values are `none`, `partial`, `complete`, and `notApplicable`.

Disc Time
The value of **ciscoDlswUpTime** when **ciscoDlswTConnOperState** last entered the `disconnected` state.

Disc Reason
Signifies the reason that either prevented the transport connection from entering the connected state, or caused the transport connection to enter the disconnected state. Possible values are `other`, `capExFailed`, `transportLayerDisc`, `operatorCommand`, `lastCircuitDiscd`, and `protocolError`.

Disc Active Cir
The number of circuits active (not in the DISCONNECTED state) at the time the transport connection was last disconnected. This value is zero if the transport connection has never been connected.

In Data Pkts
The number of Switch-to-Switch Protocol (SSP) messages of type DGRMFRAME, DATAFRAME, or INFOFRAME received on this transport connection.

Out Data Pkts
The number of Switch-to-Switch Protocol (SSP) messages of type DGRMFRAME, DATAFRAME, or INFOFRAME transmitted on this transport connection.

In Data Octets
The number octets in Switch-to-Switch Protocol (SSP) messages of type DGRMFRAME, DATAFRAME, or INFOFRAME received on this transport connection. Each message is counted starting with the first octet following the SSP message header.

Out Data Octets
The number octets in Switch-to-Switch Protocol (SSP) messages of type DGRMFRAME, DATAFRAME, or INFOFRAME transmitted on this transport connection. Each message is counted starting with the first octet following the SSP message header.

In Cntl Pkts
The number of Switch-to-Switch Protocol (SSP) messages received on this transport connection which were not of type DGRMFRAME, DATAFRAME, or INFOFRAME.

Out Cntl Pkts
The number of Switch-to-Switch Protocol (SSP) messages of transmitted on this transport connection which were not of type DGRMFRAME, DATAFRAME, or INFOFRAME.

CU Rex Sents
The number of CanUReach_ex messages sent on this transport connection.

IC Rex Rcvds
The number of ICanReach_ex messages received on this transport connection.

CU Rex Rcvds
The number of CanUReach_ex messages received on this transport connection.

IC Rex Sents
The number of ICanReach_ex messages sent on this transport connection.

N Qex Sents
The number of NetBIOS_NQ_ex (NetBIOS Name Query-explorer) messages sent on this transport connection.

N Rex Rcvds
The number of NETBIOS_NR_ex (NetBIOS Name Recognized-explorer) messages received on this transport connection.

N Qex Rcvds
The number of NETBIOS_NQ_ex messages received on this transport connection.

N Rex Sents
The number of NETBIOS_NR_ex messages sent on this transport connection.

Cisco DLSW Transport Connection TCP Config View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Transport Connections > TCP Configuration**.*

This view provides the **Dlsw TConn TCP Config Table** which defines the TCP transport connections that will be either initiated by or accepted by this DSLw. It augments the entries in Dlsw TConn Config Table (Page 129) whose domain is **ciscoDlswTCPDomain**. This table contains the following information.

Index
The index to the conceptual row of the table.

Keep Alive
The time in seconds between TCP keepAlive messages when no traffic is flowing. Zero signifies no keepAlive protocol. Changes take effect only for new TCP connections.

Tcp Connections
The preferred number of TCP connections within a TCP transport connection. The actual number used is negotiated at capabilities exchange time. Changes take effect only for new transport connections.

Max Segment
This is the number of bytes that this node is willing to receive over the read TCP connection(s). Changes take effect for new transport connections.

Cisco DLSW Transport Connection TCP Operation View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Transport Connections > TCP Operation**.*

This view provides the **Dlsw TConn TCP Oper Table** which is a list of TCP transport connections. It contains the following information.

Index
The index to the conceptual row of the table.

Keep Alive
The time in seconds between TCP keepAlive messages when no traffic is flowing. Zero signifies no keepAlive protocol is operating.

Pref Tcp
This is the number of TCP connections preferred by this DLSw partner, as received in its capabilities exchange message.

Tcp Connections
This is the actual current number of TCP connections within this transport connection.

Cisco DLSW Interface View

Access: *From the Icon Subviews menu for the CiscoDLSWApp Application icon, select **Interface**.*

This view provides the **Dlsw If Table** which is the list of interfaces on which DLSw is active. It contains the following information.

Index
A unique value for each interface.

Row Status
Used to create or delete the row entry in the ciscoDlswIfTable following the RowStatus textual convention. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Virtual Segment
The segment number that uniquely identifies the virtual segment to which this DLSw interface is connected. Current source routing protocols limit this value to the range 0 - 4095. (The value 0 is used by some management applications for special test cases.) A value of 65535 signifies that no virtual segment is assigned to this interface. For instance, in a non-source routing environment, segment number assignment is not required.

Sap List
The SAP list indicates which SAPs are allowed to be data link switched through this interface. This list has the same format described for *Sap List* (Page 131).

This implementation of DLSw does not maintain a SAP list per interface. To limit traffic based upon the SAP, interface access-lists should be applied, and their associated mib objects consulted. The default value `'ffffffffffffffffffffffffffffffff'h` indicates support for all SAPs.

Cisco DLSW Dir MAC Cache View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Directory > MAC Cache**.*

This view provides the *Dlsw Dir MAC Table* and the following information.

Mac Entries
The current total number of entries in the *Dlsw Dir MAC Table*.

Cache Hits
The number of times a cache search for a particular MAC address resulted in success.

Cache Misses
The number of times a cache search for a particular MAC address resulted in failure.

Dlsw Dir MAC Table

This table contains the locations of MAC addresses. These MAC addresses could be either verified or not verified, local or remote, and configured locally or learned from either Capabilities Exchange messages or directory searches.

Index
Uniquely identifies a conceptual row of this table.

Mac
The MAC address, together with the *Mask*, specifies a set of MAC addresses that are defined or discovered through an interface or partner DLSw nodes.

Mask
The MAC address mask, together with the *Mac*, specifies a set of MAC addresses that are defined or discovered through an interface or partner DLSw nodes. The default value is `'ffffffffffff'h`.

Entry Type
The cause of the creation of this conceptual row. Rows can be created by one of the following three

methods: (1), user configured, including via management protocol set operations, configuration file, command line or equivalent methods; (2), learned from the partner DLSw Capabilities Exchange messages; or (3), dynamic, e.g., learned from ICanReach messages, or LAN explorer frames. Since only individual MAC addresses can be dynamically learned, dynamic entries will all have a mask of all FFs.

The public versus private distinction for user-configured resources applies only to local resources (UC remote resources are private), and indicates whether that resource should be advertised in capabilities exchange messages sent by this node. Possible values are `other`, `userConfiguredPublic`, `userConfiguredPrivate`, `partnerCapExMsg`, and `dynamic`.

Location Type
The location of the resource (or a collection of resources using a mask) of this conceptual row is either `local` (the resource is reachable via an interface) or `remote` (the resource is reachable via a partner DLSw node or a set of partner DLSw nodes). Possible values are `other`, `local`, and `remote`.

Location
Identifies the location of the MAC address (or the collection of MAC addresses.)

Status
This value specifies whether DLSw currently believes the MAC address to be accessible at the specified location. The value `notReachable` allows a configured resource definition to be taken out of service when a search to that resource fails (avoiding a repeat of the search). Possible values are `unknown`, `reachable`, and `notReachable`.

LF Size
The largest size of the MAC INFO field (LLC header and data) that a circuit to the MAC address can carry through this path. The default value is `lfs65535`. Other possible values are listed in Table 15.

Row Status
Used to create or delete the row entry in the **Dlsw Dir Mac Table** following the RowStatus textual convention. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Cisco DLSW Dir NBIOS Cache View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Directory > NBIOS Cache**.*

This view provides the *Dlsw Dir NBIOS Table* and the following information.

NB Entries
The current total number of entries in the **Dlsw Dir NBIOS Table**.

NB Cache Hits
The number of times a cache search for a particular NetBIOS name resulted in success.

NB Cache Misses
The number of times a cache search for a particular NetBIOS name resulted in failure.

Dlsw Dir NBIOS Table

This table contains locations of NetBIOS names. They could be either verified or not verified, local or remote, and configured locally or learned from either Capabilities Exchange messages or directory searches.

NB Index
Uniquely identifies a conceptual row of this table.

NB Name
The NetBIOS name (including “any char” and “wildcard” characters) specifies a set of NetBIOS names that are defined or discovered through an interface or partner DLSw nodes.

NB Name Type
Whether ciscoDlswDirNBName represents an (or a set of) individual or group NetBIOS name(s). Possible values are `unknown`, `individual`, and `group`. The default value is `unknown`.

NB Entry Type
The cause of the creation of this conceptual row. Rows can be created by one of the following three methods: (1), user configured, including via management protocol set operations, configuration file, command line, or equivalent methods, (2), learned from the partner DLSw Capabilities Exchange messages, or (3), dynamic, e.g., learned from ICanReach messages, or test frames. Since only actual NetBIOS names can be dynamically learned, dynamic entries will not contain any char or wildcard characters.

The public versus private distinction for user-configured resources applies only to local resources (UC remote resources are private), and indicates whether that resource should be advertised in capabilities exchange messages sent by this node. Possible values are `other`,

userConfiguredPublic, userConfiguredPrivate, partnerCapExMsg, and dynamic. The default value is userConfiguredPublic.

NB Location Type
The location of the resource (or a collection of resources using any char/wildcard characters) of this conceptual row is either (1) local - the resource is reachable via an interface, or (2) remote - the resource is reachable via a partner DLSw node (or a set of partner DLSw nodes). Possible values are other, local, and remote. The default value is local.

NB Location
Identifies the location of the NetBIOS name or the set of NetBIOS names.

NB Status
Specifies whether DLSw currently believes the NetBIOS name to be accessible at the specified location. The value notReachable allows a configured resource definition to be taken out of service when a search to that resource fails (avoiding a repeat of the search). Possible values are unknown, reachable, notReachable. The default value is unknown.

NBLF Size
The largest size of the MAC INFO field (LLC header and data) that a circuit to the NB name can carry through this path. The default value is lfs65535. Other possible values are listed in Table 15.

NB Row Status
Used to create or delete the row entry in the **Dlsw Dir NBIOS Table** following the RowStatus textual convention. Possible values are active, notInService, notReady, createAndGo, createAndWait, and destroy.

Cisco DLSW Dir Location View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Directory > Locate**.*

This view provides the *Dlsw Dir Locate Mac Table* and the *Dlsw Dir Locate NBIOS Table*, both described below.

Dlsw Dir Locate Mac Table

This table is used to retrieve all entries in the *Dlsw Dir MAC Table* (Page 139) that match a given MAC address, in the order of the best matched first, the second best matched second, and so on. This table contains the following fields.

Index
The first part of this value is the MAC address of interest, and the second part is the order in the list of all entries that match the MAC address.

Mac Location
Points to the entry in the *Dlsw Dir MAC Table* (Page 139).

Dlsw Dir Locate NBIOS Table

This table is used to retrieve all entries in the *Dlsw Dir NBIOS Table* (Page 141) that match a given NetBIOS name, in the order of the best matched first, the second best matched second, and so on. This table contains the following fields.

Index
The first part of this value is the NetBIOS name of interest, and the second part is the order in the list of all entries that match the NetBIOS name.

NBIOS Location
Points to the entry in the *Dlsw Dir NBIOS Table* (Page 141).

Cisco DLSW Circuit View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Circuit**.*

This view provides the *Dlsw Circuit Table* (Page 144), and the two fields described below.

Active Circuits
The current number of circuits in the *Dlsw Circuit Table* (Page 144) that are not in the disconnected state.

Circuit Creates
The total number of entries ever added to *Dlsw Circuit Table*, or reactivated upon exiting `disconnected` state.

Dlsw Circuit Table
This table is the circuit representation in the DLSw entity. Virtual data links are used to represent any internal end stations. There is a conceptual row associated with each data link. Thus, for circuits without an intervening transport connection, there are two conceptual rows for each circuit.

The table consists of the circuits being established, and as an implementation option, circuits that have been disconnected. For circuits carried over transport connections, an entry is created after the CUR_cs was sent or received. For circuits between two locally attached devices, or internal virtual MAC addresses, an entry is created when the equivalent of CUR_cs sent/received status is reached.

End station 1 (S1) and End station 2 (S2) are used to represent the two end stations of the circuit. S1 is always an end station which is locally attached. S2 may be locally attached or remote. If it is locally attached, the circuit will be represented by two rows indexed by (A, B) and (B, A) where A & B are the relevant MACs/SAPs. This table contains the following information.

Index
The index to the conceptual row of the table.

S1 Mac
The MAC Address of End Station 1 (S1) used for this circuit.

S1 Sap
The SAP at End Station 1 (S1) used for this circuit.

S1 If Index
The IfEntry index of the local interface through which S1 can be reached.

S1 Dlc Type
The DLC protocol in use between the DLSw node and S1. Possible values are `other`, `na`, `llc`, `sdlc`, and `qllc`.

S1 Route Info
If source-route bridging is in use between the DLSw node and S1, this is the routing information field describing the path between the two devices. Otherwise, the value will be an octet string of zero length.

S1 Circuit Id
The Circuit ID assigned by this DLSw node to this circuit. The first four octets are the DLC port Id,

and the second four octets are the Data Link Correlator. If the DLSw SSP was not used to establish this circuit, the value will be a string of zero length.

S1 Dlc
Points to a conceptual row of the underlying DLC MIB, which could either be the standard SDLC or LLC MIBs, or an enterprise-specific DLC MIB.

S2 Mac
The MAC Address of End Station 2 (S2) used for this circuit.

S2 Sap
The SAP at End Station 2 (S2) used for this circuit.

S2 Location
Possible values are `other`, `internal`, `remote`, and `local`. The location of End Station 2 (S2). If the location of End Station 2 is local, the interface information will be available in the conceptual row whose S1 and S2 are the S2 and the S1 of this conceptual row, respectively.

S2T Domain
If the location of End Station 2 is remote, this value is the transport domain of the transport protocol the circuit is running over. Otherwise, the value is 0.0.

S2T Address
If the location of End Station 2 is remote, this field contains the address of the partner DLSw. Otherwise, it will contain an octet string of zero length.

S2 Circuit Id
The Circuit ID assigned to this circuit by the partner DLSw node. The first four octets are the DLC port Id, and the second four octets are the Data Link Correlator. If the DLSw SSP was not used to establish this circuit, the value will be a string of zero length.

Origin
Specifies which of the two end stations initiated the establishment of this circuit. Possible values are `s1` and `s2`.

Entry Time
The value of **ciscoDlswUpTime** when this circuit table conceptual row was created.

State Time
The value of **ciscoDlswUpTime** when this circuit entered the current state.

State
The current state of this circuit. While all of the specified values may be returned from a GET operation, the only SETable value is `disconnectPending`. When this value is set,

DLSw should perform the appropriate action given its previous state (e.g., send HALT_DL if the state was `connected`) to bring the circuit down to the `disconnected` state. Both the partner DLSw and local end station(s) should be notified as appropriate. Possible values are `disconnected`, `circuitStart`, `resolvePending`, `circuitPending`, `circuitEstablished`, `connectPending`, `contactPending`, `connected`, `disconnectPending`, `haltPending`, `haltPendingNoack`, `circuitRestart`, and `restartPending`.

Priority
The transmission priority of this circuit as understood by this DLSw node. This value is determined by the two DLSw nodes at circuit startup time. If this DLSw node does not support DLSw circuit priority, the value `unsupported` should be returned. Possible values are `unsupported`, `low`, `medium`, `high`, and `highest`.

FC Send Granted Units
The number of paced SSP messages that this DLSw is currently authorized to send on this circuit before it must stop and wait for an additional flow control indication from the partner DLSw. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Send Current Wndw
The current window size that this DLSw is using in its role as a data sender. This is the value by which this DLSw would increase the number of messages it is authorized to send, if it were to receive a flow control indication with the bits specifying “repeat window”. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Recv Granted Units
The current number of paced SSP messages that this DLSw has authorized the partner DLSw to send on this circuit before the partner DLSw must stop and wait for an additional flow control indication from this DLSw. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Recv Current Wndw
The current window size that this DLSw is using in its role as a data receiver. This is the number of additional paced SSP messages that this DLSw would be authorizing its DLSw partner to send, if this DLSw were to send a flow control indication with the bits specifying “repeat window”. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Largest Recv Granted
The largest receive window size granted by this DLSw during the current activation of this circuit. This is not the largest number of messages granted at any time, but the largest window size as represented by FCIND operator bits. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Largest Send Granted
The largest send (with respect to this DLSw) window size granted by the partner DLSw during the current activation of this circuit. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Halve Wndw Sents
The number of Halve Window operations this DLSw has sent on this circuit, in its role as a data receiver. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Reset Op Sents
The number of Reset Window operations this DLSw has sent on this circuit, in its role as a data receiver. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Halve Wndw Rcvds
The number of Halve Window operations this DLSw has received on this circuit, in its role as a data sender. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

FC Reset Op Rcvds
The number of Reset Window operations this DLSw has received on this circuit, in its role as a data sender. The value zero should be returned if this circuit is not running the DLSw pacing protocol.

Disc Reason Local
The reason why this circuit was last disconnected, as seen by this DLSw node. Possible values are `endStationDiscRcvd`, `endStationDlcError`, `protocolError`, `operatorCommand`, `haltDlRcvd`, `haltDlNoAckRcvd`, and `transportConnClosed`.

Disc Reason Remote
The generic reason code why this circuit was last disconnected, as reported by the DLSw partner in a HALT_DL or HALT_DL_NOACK. If the partner does not send a reason code in these messages, or the DLSw implementation does not report receiving one, the value `unknown` is returned. Possible values are `unknown`, `endStationDiscRcvd`, `endStationDlcError`, `protocolError`, and `operatorCommand`.

Disc Reason Remote Data
Implementation-specific data reported by the DLSw partner in a HALT_DL or HALT_DL_NOACK, to help specify how and why this circuit was last disconnected. If the partner does not send this data in these messages, or the DLSw implementation does not report receiving it, a string of zero length is returned.

Cisco DLSW SDLC View

Access: *From the **Icon Subviews** menu for the CiscoDLSWApp Application icon, select **Circuit**.*

This view provides the *Dlsw LS Table* and the field described below.

Number of SDLC LS Entries
The number of entries in the *Dlsw LS Table*.

Dlsw LS Table

This table defines the virtual MAC addresses for those SDLC link stations that participate in data link switching and contains the following information.

Index
The index of this table is the **ifIndex** value for the SDLC port which owns this link station and the poll address of the particular SDLC link station.

Local Mac
The virtual MAC address used to represent the SDLC-attached link station to the rest of the DLSw network.

Local Sap
The SAP used to represent this link station.

Local Block Num
The block number is the first three digits of the node_id, if available. These 3 hexadecimal digits identify the product and are not configurable.

Local Id Num
The ID number is the last 5 digits of the node_id, if available. These 5 hexadecimal digits are administratively defined and combined with the 3 digit block number form the node_id. This node_id is used to identify the local node and is included in SNA XIDs.

Remote Mac
The MAC address to which DLSw should attempt to connect this link station. If this information is not available, a value of zero for this object should be returned.

Remote Sap
The SAP of the remote station to which this link station should be connected. If this information is not available, a length of zero for this object should be returned.

Row Status
Used to create a new row or delete an existing row in this table. Possible values are `active`, `notInService`, `notReady`, `createAndGo`, `createAndWait`, and `destroy`.

Cisco HSRP Application

This application (CiscoHSRPApp) supports the CISCO-HSRP-MIB. This MIB module lets you manage HSRP (Hot Standby Router Protocol) groups. HSRP provides a means of setting up redundant router connections among several Cisco routers. HSRP designates one router as the active router and holds all of the other routers in the HSRP group in reserve. If the active router fails, another router in the HSRP group immediately takes over. The HSRP group is represented by a virtual IP address which does not change. Only the IP address of the active and standby router(s) changes.

The Cisco HSRP application provides access to the following views:

- *Cisco HSRP Group Table View* (Page 150)
- *Cisco HSRP Group Tracked Interface Table View* (Page 153)
- *Cisco Secondary HSRP IP Address Table View* (Page 154)
- *Cisco HSRP Physical Interface Configuration Table View* (Page 155)

Cisco HSRP Group Table View

Access: *From the **Icon Subviews** menu for the CiscoHSRPApp Application icon, select **HSRP Group Table**.*

This view provides the *HSRP Group Table* (Page 150) and a *Config Timeout* field, described below.

Note: The Cisco Router device model provides a means of representing an HSRP group in SPECTRUM by suppressing duplicate MAC address alarms when an HSRP virtual IP is modeled. This avoids any confusion and the inconvenience of an alarm when modeling routers that are part of an HSRP group.

Config Timeout
The amount of time in minutes a row in the HSRP Group Table can remain in a state other than active before being timed out.

HSRP Group Table

This table contains the following information on each HSRP group for each interface. Double-clicking an entry in this table opens a Cisco HSRP Group View which contains the same information for and lets you configure that entry.

IF Index
The interface index value.

HSRP Group
This field along with the ifIndex of a particular interface uniquely identifies an HSRP group. Group numbers 0, 1, and 2 are the only valid group numbers for Token Ring interfaces. For other media types, numbers range from 0 to 255. Each interface has its own set of group numbers. There is no relationship between the groups configured on different interfaces. Using a group number on one interface does not preclude using the same group number on a different interface. For example, there can be a group 1 on an Ethernet and a group 1 on Token Ring.

Authentication
An unencrypted authentication string which is carried in all HSRP messages. An authentication string mismatch prevents a router interface from learning the designated IP address or HSRP timer values from other HSRP-enabled routers with the same group number. The function of this field is not to supply any sort of security-like authentication but rather to confirm that what's happening is what's intended.

Priority
Helps to select the active and the standby routers. The router with the highest priority is selected as

the active router. In the priority range of 0 to 255, 0 is the lowest priority and 255 is the highest priority.

If two (or more) routers in a group have the same priority, the one with the highest IP address of the interface is the active router. When the active router fails to send a Hello message within a configurable period of time, the standby router with the highest priority becomes the active router.

A router with highest priority will only attempt to overthrow a lower priority active router if it is configured to preempt. But, if there is more than one router which is not active, the highest priority non-active router becomes the standby router.

Preempt

A value of `True` indicates that the current router should attempt to overthrow a lower priority active router and attempt to become the active router. A value of `False` indicates the router will become the active router only if there is no such router (or if an active router fails).

Preempt Delay

The time difference between a router power up and the time it can actually start preempting the currently active router.

When a router first comes up, it doesn't have a complete routing table. If it's configured to preempt, then it will become the Active router, but it will not be able to provide adequate routing services. The solution to this is to allow for a configurable delay before the router actually preempts the currently active router.

Use Configured Timers

HSRP routers learn a group's Hellotime or Holdtime from hello messages.

The Hellotime is used to determine the frequency of generating hello messages when this router becomes the active or standby router. The Holdtime is the interval between the receipt of a Hello message and the presumption that the sending router has failed.

If this field is `True`, the *Configured Hello Time* (Page 152) and *Configured Hold Time* (Page 152) will be used. If it is `False`, these values are learned.

Configured Hello Time
If *Use Configured Timers* (Page 151) is “true”, this value is used when this router is an active router. Otherwise, the Hellotime learned from the current active router is used. All routers on a particular LAN segment must use the same Hellotime.

Configured Hold Time
If *Use Configured Timers* (Page 151) is “true”, this value is used when this router is an active router. Otherwise, the Holdtime learned from the current active router is used. All routers on a particular LAN segment should use the same Holdtime. Also, the Holdtime should be at least three times the value of the Hellotime and must be greater than the Hellotime.

Learned Hello Time
If the Hellotime is not configured on a router, it can be learned from the Hello messages from the active router, provided the Hello message is authenticated. If the Hellotime is not learned from a Hello message from the active router and it is not manually configured, a default value of `3 seconds` is recommended.

Learned Hold Time
If the Holdtime is not configured on a router, it can be learned from the Hello message from the active router. Holdtime should be learned only if the Hello message is authenticated. If the Holdtime is not learned and it is not manually configured, a default value of `10 seconds` is recommended.

Virtual IP Address
The primary virtual IP address used by this group. If this address is configured, this value is used. Otherwise, the agent will attempt to discover the virtual address through a discovery process (which scans the hello messages).

Use Configured Virtual IP
If this field is `True`, **Virtual IP Address** was a configured one. Otherwise, it indicates that **Virtual IP Address** was learned.

Active Router
IP Address of the currently active router for this group.

Standby Router
IP Address of the current standby router for this group.

Standby State
The current HSRP state of this group on this interface. Possible values are `initial`, `learn`, `listen`, `speak`, `standby`, and `active`.

Virtual MAC Address
Mac Addresses used are as specified in RFC 2281. For Ethernet and FDDI interfaces, a MAC address will be in the range 00:00:0c:07:ac:00 through 00:00:0c:07:ac:ff. The last octet is the hexadecimal equivalent of **Hsrp Grp Number** (0-255). Some Ethernet and FDDI interfaces allow a unicast MAC address for each HSRP group. Certain Ethernet chipsets (LANCE Ethernet, VGANYLAN and QUICC Ethernet) only support a single Unicast Mac Address. In this case, only one HSRP group is allowed. For Token Ring interfaces, the following three MAC addresses are permitted (functional addresses):

C0:00:00:01:00:00
C0:00:00:02:00:00
C0:00:00:04:00:00

Row Status
The control that allows modification, creation, and deletion of entries.

Cisco HSRP Group Tracked Interface Table View

Access: *From the **Icon Subviews** menu for the CiscoHSRPApp Application icon, select **Tracked Interfaces Info**.*

IF Index
The interface index value.

HSRP Group
This field along with the ifIndex of a particular interface uniquely identifies an HSRP group. Group numbers 0, 1 and 2 are the only valid group numbers for Token Ring interfaces. For other media types, numbers range from 0 to 255. Each interface has its own set of group numbers. There is no relationship between the groups configured on different interfaces. Using a group number on one interface does not preclude using the same group number on a different interface. For example, there can be a group 1 on an Ethernet and a group 1 on Token Ring.

Tracked IF
The ifIndex of the tracked interface.

Priority
Priority of the tracked interface for the corresponding { **ifIndex**, **cHsrpGrpNumber** } pair. In the range of 0 to 255, 0 is the lowest priority and 255 is the highest. When a tracked interface is unavailable, the **cHsrpGrpPriority** of the router is decreased by the value of this field instance. If the **cHsrpGrpPriority** is less than the **cHsrpExtIfTrackedPriority**, then the HSRP priority becomes 0. This allows a standby router to be configured with a priority such that if the currently active router's priority is lowered because the tracked interface goes down, the standby router can take over.

Row Status
The control that allows modification, creation, and deletion of entries.

Cisco Secondary HSRP IP Address Table View

Access: *From the **Icon Subviews** menu for the CiscoHSRPApp Application icon, select **Secondary HSRP IP Address Table**.*

Column headings are as follows.

IF Index
The interface index value.

HSRP Group
This field along with the **ifIndex** of a particular interface uniquely identifies an HSRP group. Group numbers 0, 1, and 2 are the only valid group numbers for Token Ring interfaces. For other media types, numbers range from 0 to 255. Each interface has its own set of group numbers. There's no relationship between the groups configured on different interfaces. Using a group number on one interface doesn't preclude using the same group number on a different interface. For example, there can be a group 1 on an Ethernet and a group 1 on Token Ring.

Secondary Address
A secondary IP Address for the {**ifIndex**, **cHsrpGrpNumber**} pair. A primary address must exist before a secondary address for the same {**ifIndex**, **cHsrpGrpNumber**} pair can be created.

Row Status
The control that allows modification, creation, and deletion of entries.

Cisco HSRP Physical Interface Configuration Table View

Access: *From the **Icon Subviews** menu for the CiscoHSRPApp Application icon, select **Physical Interface Configuration**.*

Column headings are as follows.

IF Index
The interface index value.

Use Burned In Address
If set to `True`, the HSRP Group MAC Address for all groups on this interface will be the burned-in-address. Otherwise, this will be determined by **Hsrp Group Number**. In case of sub-interfaces, Use BIA applies to all sub-interfaces on an interface and to all groups on those sub-interfaces.

Row Status
The control that allows modification, creation, and deletion of entries.

Performance Views

This section provides brief descriptions of the Performance views available for models of Cisco Router devices in SPECTRUM. For details concerning this view, refer to the ***SPECTRUM Views*** documentation.

The following performance views are described in this section:

- *Performance View*
- *Device Performance View* (Page 157)

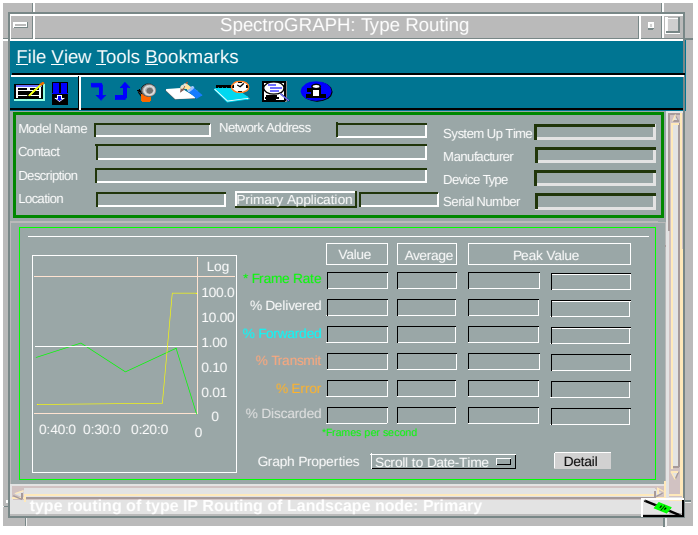
Performance View

Access: *From the **Icon Subviews** menu for the Device icon, select **Performance.***

Performance views display performance statistics in terms of a set of transmission attributes, e.g., cell rates, frame rates, % error, etc. A typical view is shown in Figure 7. The instantaneous condition of each transmission attribute is recorded in a graph. The statistical information for each attribute is presented in the adjacent table.

Generally, you determine performance at the device level through Performance views accessed from the Device and Application icons. You determine performance at the port/interface level through Performance views accessed from Interface icons.

Figure 7: Performance View



Device Performance View

Access: *From the* ***Icon Subviews*** *menu for the Device icon, select* ***Device Performance.***

Note:

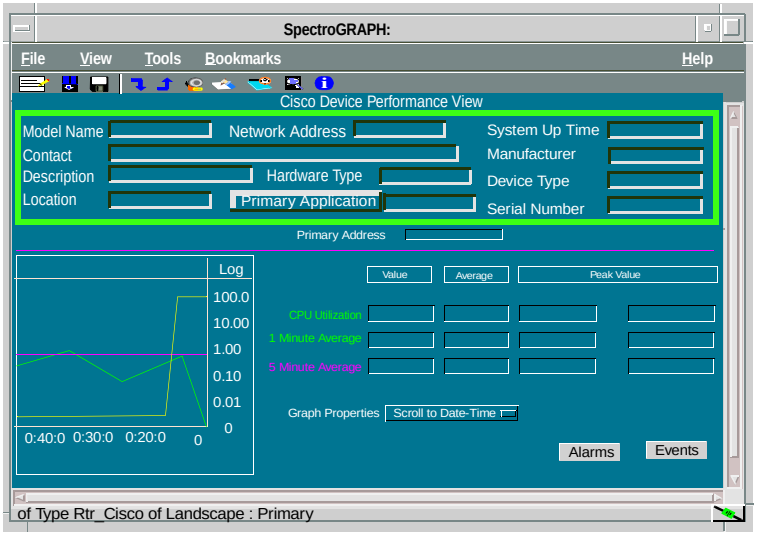
For devices with firmware greater than 12.0, selecting Device Performance opens the *Cisco Processes CPU Statistics Table View* (Page 158).

This view (Figure 8) includes both a graph and a table that show current, average, and peak values for the following performance statistics:

- CPU Utilization
- 1 Minute Average
- 5 Minute Average

The view also provides button access to the Enterprise Alarm Manager and the Event Log.

Figure 8: Device Performance View



Cisco Processes CPU Statistics Table View

This table displays overall CPU statistics. Column headings are as follows.

CPU
An index that uniquely represents a CPU (or group of CPUs) whose load information is reported by a row in this table. This index is assigned arbitrarily by the engine and is not saved over reboots.

Physical Index
The physical entity for which the CPU statistics in this entry are maintained. The physical entity can be a CPU chip, a group of CPUs, a CPU card etc. The exact type of this entity is described by its **entPhysicalVendorType** value. If the CPU statistics in this entry correspond to more than one physical entity (or to no physical entity), or if the entPhysicalTable is not supported on the SNMP agent, the value of this field must be zero.

5 Sec Busy %
The overall CPU busy percentage in the last 5 second period.

1 Min Busy %
The overall CPU busy percentage in the last 1 minute period.

5 Min Busy %
The overall CPU busy percentage in the last 5 minute period.

Configuration Views

This section describes the Configuration views available for models of the Cisco Router devices in SPECTRUM.

Configuration views let you see and modify current settings for the modeled device and its interfaces, ports, and applications. The following Configuration view is available for models of Cisco Router devices:

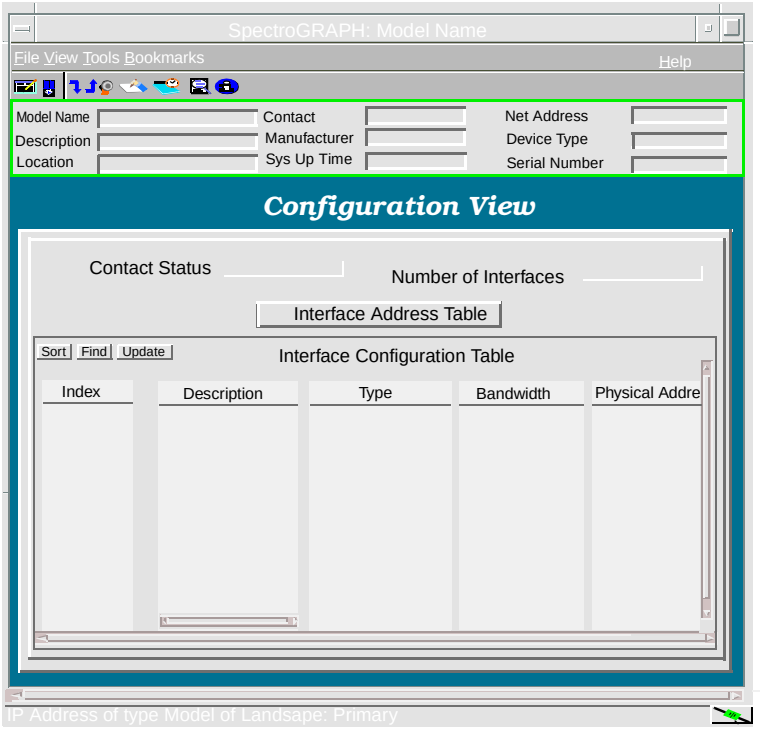
- *Device Configuration View*

Device Configuration View

Access: *From the* ***Icon Subviews*** *menu for the Device icon, select* ***Configuration****.*

A typical Device Configuration view is shown in Figure 9. Generally, this view includes a few fields that display device information as well as an Interface Configuration Table that lists interface parameters, some of which can be changed (see ***SPECTRUM Views***). Some Device Configuration views include one or more buttons that provide access to device-specific configuration information. These are described below.

Figure 9: Device Configuration View



Discover/Reconfigure Control

Accesses the *Redundancy and Model Reconfiguration Options View*.

IF Address Translation

Refer to the ***SPECTRUM Views*** documentation.

Memory Pool Monitor

Accesses the *Cisco Memory Pool Monitor Table View* (Page 161).

Config Copy Table

Accesses the *Cisco Config-Copy Table View* (Page 162).

Running Configuration Changes

Accesses the *Cisco Running Config Event/Alarm Configuration View* (Page 165).

Redundancy and Model Reconfiguration Options View

Access: *In the* ***Device Configuration View,*** *click the* ***Discover/Reconfigure Control*** *button.*

This view allows you to enable redundant addresses, have SPECTRUM notify you of a redundancy update, and reconfigure aspects of your network connections.

Preferred Addresses

This button opens the Preferred Addresses dialog box which allows you to select the redundant preferred address for the device.

Redundancy Administrative Status

Set this button to “Enabled” to cause SPECTRUM to update this model with an address from the Redundant Preferred Address list when the primary address is not accessible.

Generate Redundancy Alarms

Set this button to “True” to cause SPECTRUM to generate an alarm when a redundant address is selected.

Automatically Reconfigure Interfaces

Set this button to “True” to cause SPECTRUM to monitor the number of interfaces for this device. If a change is detected by SPECTRUM, the

interfaces displayed in SPECTRUM are updated to reflect the change.

Create Sub-Interfaces
Set this button to determine if SPECTRUM should model the device's sub-interfaces. If set to "True," these models will be displayed in the Sub-Interface view of the Physical Interface model.

Reconfigure due to LINK UP/Down events
Set this button to "True" to cause SPECTRUM to verify the interfaces displayed when a LINK UP or LINK DOWN event is received.

Topologically Relocate Model
Set this button to "True" to allow SPECTRUM to relocate the model to a different topological location as part of the AutoDiscovery process.

Device Discovery after Reconfiguration
Set this button to "True" to cause SPECTRUM to verify the interfaces displayed after a model reconfiguration occurs.

Reconfigure Model

This button does a complete re-read of the device and its ports. The SpectroSERVER information for this device will be updated if any of the port addresses have been changed or removed, or if the port type has been changed.

Discover LANs

This button discovers the devices that are connected to the ports for this device. Clicking on this button will create all LANS which are defined for each port.

Cisco Memory Pool Monitor Table View

This table displays memory pool monitoring entries.

Name
Displays the name assigned to a memory pool.

Alternate
Indicates whether or not this memory pool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If this has a value of zero than there is no alternate.

Valid
This indicates whether or not the remaining fields in this entry contain accurate data. If an instance of this field has a `false` value, the values of this row may contain inaccurate information.

Used
Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.

Free
The number of bytes from the memory pool that are currently unused on the managed device.

Largest Free
Indicates the largest number of contiguous bytes from the memory pool that are currently unused on the managed device.

Cisco Config-Copy Table View

A config-copy operation is a request to copy a configuration file of an SNMP Agent running Cisco's IOS software. There are several ways in which this can be done: copying to or from the net (via a protocol like tftp, ftp, or rcp), copying running configurations and vice-versa, or by copying a running or startup config to a file to the local IOS file system and vice versa.

This view displays the **ccCopyTable** which provides the following information.

Index
Specifies a unique entry in the **ccCopyTable**.

Protocol
The protocol to be used for any copy. Will default to tftp if not specified. If the copy operation occurs locally on the SNMP agent, this value may be ignored by the implementation.

Source File Type
The type of file to copy from. Either the Source File Type or the Dest File Type (or both) must be of type runningConfig or startupConfig. Also, the Source File Type must be different from the Dest File Type. If the Source File Type has the value of networkFile, the Server Address and File Name must also be created, and these 3 values together (Source File Type, Server Address, File Name) will uniquely identify the source file. Possible types are `networkFile`, `iosFile`, `startupConfig`, `runningConfig`, and `terminal`.

If the Source File Type is iosFile, the File Name must also be created, and the 2 values together (Source File Type, File Name) will uniquely identify the source file.

Dest File Type
The Destination File Type, which is the type of file to copy to. Either the Source File Type or the Dest File Type (or both) must be of type running Config or startupConfig. Also, the Source File Type must be different from the Dest File Type. If the Dest File Type has the value of network File, the Server

Address and File Name must also be created, and these three values together (Dest File Type, Server Address, File Name) will uniquely identify the destination file. If the Dest File Type is iosFile, the File Name must also be created, and the two values together (Dest File Type, File Name) will uniquely identify the destination file. Possible types are `networkFile`, `iosFile`, `startupConfig`, `runningConfig`, and `terminal`.

Server Address
The IP address of the TFTP server from (or to) which to copy the configuration file. This value must be created when either the Source File Type or Dest File Type has the value networkFile. Values of 0.0.0.0 or FF.FF.FF.FF. for Server Address are not allowed.

File Name
The file name (including the path, if applicable) of the file. This value must be created when either the Source File or Dest File Type has the value networkFile or iosFile.

User Name
Remote user name for copy via rcp protocol. This value must be created when the Protocol is rcp or ftp. If the protocol is rcp, it will override the remote user name configured through the rcmd remote-username configuration command. The remote user name is sent as the server user-name in an rcp command request sent by the system to a remote rcp server.

User Password
Password used by ftp for copying a file to/from an ftp server. This value must be created when the Protocol is ftp. Reading it returns a zero-length string for security reasons.

Notification On Completion
Specifies whether or not a Notification on Completion should be issued on completion of the tftp transfer. If such a notification is desired, it is the responsibility of the management entity to ensure that the SNMP administrative model is configured in such a way as to allow the notification to be delivered.

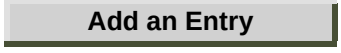
State
The state of this config-copy request. The value of this field is instantiated only after the row has been instantiated, i.e., after the Row Status has been made active.

Time Started
The time the Copy State last transitioned to running, or 0 if the state has never transitioned to running (for e.g., stuck in waiting state). This field is instantiated only after the row has been instantiated.

Time Completed
The time the Copy State last transitioned from running to successful or failed states. This field is instantiated only after the row has been instantiated. Its value will remain 0 until the request has completed.

Fail Reason
The reason why the config-copy operation failed. This field is instantiated only when the Copy State for this entry is in the failed state.

Row Status
The status of this table entry. Once the entry status is set to active, the associated entry cannot be modified until the request completes (Copy State transitions to successful or failed state).



This button opens the Add a Cisco Copy Config Entry view which allows you to add an entry to the Cisco Config-Copy Table (Page 162).

Cisco Running Config Event/Alarm Configuration View

Access: *In the Configuration View, click the* ***Running Configuration Changes*** *button.*

This view lets you set when the attribute **ccmHistoryRunningLastChanged** is checked. This attribute tells you if and when the configuration has changed. This view also lets you set the generation of either an event or an alarm if it does change. Alarms and events can be set to apply to just the current model or all models of this model type, as described below.

Note: If **ccmHistoryRunningLastChanged** does change, the user may want to rediscover applications.

Hour to Run Cron Job:

This button allows you to select the hour of day to run the cron job.

Generate Event for This Model

This button allows you to select if you wish to generate an event for this model. Valid options are `True` and `False`.

Generate Event For All Models Of This Model Type

This button allows you to select if you wish to generate an event for all models of this model type. Valid options are `True` and `False`.

Generate Alarm For This Model

This button allows you to select if you wish to generate an alarm for this model. Valid options are `True` and `False`.

Generate Alarm For All Models Of This Model Type

This button allows you to select if you wish to generate an alarm for all models of this model type. Valid options are `True` and `False`.

Running Configuration Was last Changed At:
The date and time the running configuration was last updated.

Syslog Trap Support

This section describes the Syslog Trap Support available for the Cisco Router.

The System Message Log (syslog) protocol is used to send text messages from a Cisco Router to the Network Management Software. These messages are sent to the SPECTRUM Event Manager as SNMP traps. Syslog trap support allows the router device to identify these messages and escalate them to alarms as necessary. Syslog trap support also provides the Cisco Router model icon the capability to communicate model alarm severity information. When an alarm occurs, as indicated by the Cisco Router device icon, you will be able to observe the SPECTRUM Alarm Severity and a Syslog message will appear in the Alarm log (which can be found in the Alarm Manager View).

These Syslog messages are classified by severities that range from 0 to 7 (most severe to least severe). These messages are described in Table 17 The alarms are displayed in the Alarm Log. As these alarms are associated with the Cisco Router device model, the model icon will change color and flash depending on the severity of the alarm that it receives.

Table 17: Severity Level Code

Severity Level	Description
0	emergency-System is unusable.
1	alert- Immediate action required.
2	critical -Critical condition.
3	error- Error condition.
4	warning- Warning condition.
5	notification- normal but significant condition
6	informational- informational message only.
7	debugging- message that appears during debugging only.

The Syslog message severity is mapped to the SPECTRUM alarm severity as listed in Table 18.

Table 18: Syslog Message Severity

Alarm Severity	Color
0-1	Red
2-3	Orange
4	Yellow

Messages with an Alarm Severity of 5 through 7 typically do not generate an alarm, as they are of minor importance.

Messages are listed by the facility (hardware device, protocol, or a module or system software) that produces the messages. A facility code is an abbreviation of the facility to which the message refers to. A facility could be a specific hardware device, a protocol, or a portion of software.

Within each facility, messages are listed by the severity level, from highest (0) to lowest (7). A mnemonic is a code which uniquely identifies the message.

Each message is followed by an explanation and a recommended action. Messages appear only when

- select the destination of captured logging

the system remains operational. The following is an example of a syslog message:

```
01/01/2001,18:31:15:SYS-5-
MOD_INSERT:Module 5 has been inserted
```

The meaning of this message is as follows:

- `01/01/2001,18:31:15` is the date and time of the error (this appears if set for system log messaging).
- `SYS` is the facility type.
- `5` is the severity level, indicating that it is a normal but significant condition.
- `MOD_INSERT` is the mnemonic code that uniquely identifies the message. All mnemonics are uppercase character strings.
- `Module 5 has been inserted` is the message text which describes the condition and may contain detailed information which varies from message to message.

The System Message Log (syslog) software can save the system messages in a log file or direct them to other devices. Syslog software allows you to do the following:

- save logging information for monitoring and troubleshooting.
- select the types of logging information captured.

  information.

By default the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. Messages can be time-stamped to enhance real-time debugging and management.

Refer to the **Alarm Notification Manager** documentation for more information about the SPECTRUM Alarm Manager.

Note: This management module supports the system error messages for the Cisco IOS Release 12.1 T.

Note: The URL www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/sem121t.htm is a link to more information about Cisco Router syslog messages including a list of facility codes and of error messages with their corresponding recommended actions.

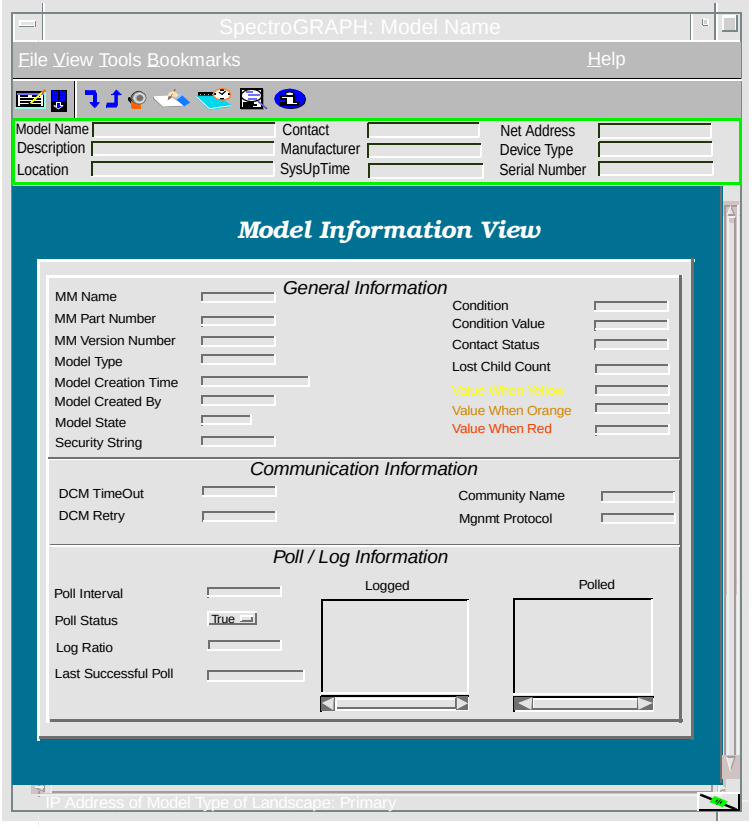
Model Information View

This section provides a brief overview of the Model Information view.

Model Information views display administrative information about devices and their applications and let you set thresholds and alarm severity for the devices.

Figure 10 shows a sample Model Information view. The layout of this view is the same for all model types in SPECTRUM but some information will vary depending on the model it defines. Refer to the ***SPECTRUM Views*** documentation for a complete description of this view.

Figure 10: Model Information View



Index

Numerics

1 Min Busy % 158
5 Min Busy % 158
5 Sec Busy % 158

A

Active Connections 129
Active Router 152
Add an Entry button 69
Add Flash Copy Operation view 63
Address 89
  Interface IP 19
  Physical (MAC) 19
Address Translation Table 20
Application icons 25
Applications Supported
  Common Applications 11
ATM Client Application 72
  ATM Link Modeling Options 74
  VCL Table 72
ATM Link Modeling Options View
  Config Interval 74
  Create Link Models 74
  Create VCL Models 74
  Option Explanations 74
  Reconfigure Now 74
ATMClientApp 72
Authentication 150
Available 62

B

B-casts Forwarded 35
BGP4 Application 30
Binary Synchronous
    Communication 35
Bootstrap, Messages 101
Broadcasts 34
BSC (Binary Synchronous
    Communication) 35
BSR 98, 99
  Address 102
  Expiry Time 102
BSTUN
  Groups View 35
  Ports View 36
  Routes View 37
Bytes 29

C

Candidate Bootstrap Router
  Preference 97
Candidate Rendezvous Point
    Table 100
  Address 101
  Group Address 100
  Group Mask 101
  Row Status 101
CBSR Preference 97
ccmHistoryRunningLastChanged 1
    65
cde Fast Table 123
cde If Table 122, 124
cde TConn Config Table 116
cde TConn Oper Table 119, 121
cde TConn Tcp Config Table 121
Chassis
  ID/Serial No. 51
  Information 41
  Type 41
Chassis Application 40
Chassis Card View 40
Chassis General Information
    View 41
  RAM Information 51
  ROM Information 51

Index

Checkpoint
  Accounting
    Button 29
    Table 29
  View Information 29
Circuit 128
CiscIPMRoutApp 87
Cisco
  Chassis
    Application Views 40
    Card View 40
    General Information View 41
  Flash
    Application Views 61
  IP Accounting Table 29
  Terminal Server
    Line View 80
    Session View 82
Cisco Chassis Card View 40
Cisco Chassis General Information View 40
Cisco DLSW Ext Node View 116
Cisco DLSW Node View 126
Cisco Interface Application 80
Cisco IPM Route Heart Beat Table
  Alert Time 95
  Count 95
  Group Address 94
  Interval 94
  Row Status 95
  Source Address 94
  Window Size 95
Cisco IPM Route Next Hop Table 93
  Address 94
  Group Address 93
  IF Index 94
  MAC Address Header 94
  Outgoing Limit 94
  Source Address 93
  Source Mask 93
Cisco IPM Route Table
  Bits/Second 92
  Connected Flag 92
  Group Address 91
  In Limit 92
  In Limit2 93
  Join Flag 93
  Last Used 92
  Local Flag 92
  Metric 92
  Metric Preference 92
  Metric2 93
  MSDP Flag 93
  Proxy Join Flag 93
  Prune Flag 91
  Register Flag 92
  RP Flag 92
  Source Address 91
  Source Mask 91
  Sparse Flag 92
  SPT Flag 92
Cisco Network Info 20
Cisco Other Info 20
Cisco PIM Objects View 102
  Invalid Join Prune Msgs Rcvd 102
  Invalid Register Msgs Rcvd 102
  Last Error Group 103
  Last Error Group Type 103
  Last Error Origin 103
  Last Error Origin Type 103
  Last Error RP 103
  Last Error RP Type 103
  Last Error Type 103
  RP Mapping Change Type 104
Cisco Router Info 20
Cisco STUN Application 37
Cisco Traffic Info 20
Cisco VPDN System Info View 104
  Denied User Total 105
  Session Total 105
  Tunnel Total 104
  Type 104, 111
Cisco VPDN Tunnel Attribute View 105
  Active Sessions 106
  Denied Users 106
  Index 105
  Local Init Conn 105
  Local Ip Addr 106
  Local Name 105
  Network Service Type 106
  Original Cause 105
  Remote Endpoint Name 105
  Remote Ip Addr 106
  Remote Name 105
  Soft Shut 106

Index

Source Ip Addr 106
Tunnel Attr State 105
Cisco VPDN Tunnel Session View 107
Bytes In 108
Bytes Out 108
Call Duration 108
Call Start Index 109
Call Start Time 109
Device Caller ID 109
Device Type 108
DS1 Chan Index 109
DS1 Port Index 109
DS1 Slot Index 109
Index 107
Modem Port Index 109
Modem Slot Index 109
Multi Link 109
Packets In 108
Packets Out 108
Tunnel State 107
User Name 107
Cisco VPDN User Failure History View 109
Dest IP 110
Fail Reason 110
Fail Time 110
Fail Type 110
Hist Count 110
Index 109
Local Init Conn 110
Local Name 110
Remote Name 110
Source IP 110
Tunnel ID 110
User ID 110
User Name 110
Cisco_Mem_App 83
CiscoChasApp 40
CiscoDLSWExtApp 111, 125
ciscoDlswstate 127
CiscoFddiApp 78
CiscoFlashApp 61
CiscoHSRPApp 149
CISCO-HSRP-MIB 149
CiscoPIMApp 95
CiscoPingApp 68
CiscoTSApp 80
CiscoVPDNApp 104
CiscoXNSApp 35
Close Busys 129
Close Idles 129
Closest Member Hops 89
Config Register 51
Config Timeout 150
Configuration Device 159
Configure a Port 12
Configure the Device 11
Configured Hello Time 152
Configured Hold Time 152
Connection_Configuration_Filter 85
CPU 158
Creating LANs 12
CsEvFormat 14

D

Description 40
Designated Router (DR) 103
Destination 29
Diff In IF Packets 88
Disconnect Reasons 55
Discover LANs 161
Discovery Application
Cache Table View 78
Interface Discovery Status Table 79
Dlsw Circuit Table 144
Dlsw Dir NBIOS Table 141
Dlsw If Table 138
DLSW TConn Config Table 129
Dlsw TConn Operation Table 132
Dlsw TConn TCP ConfigTable 137
Dlsw TConn TCP Oper Table 138
DLSW Transport Connections
Configuration 129
Operation 132
Statistics 129
dlswCircuitTable 124
DLSW-MIB 121, 122

Index

E

ECEditor 14
Echo
  Count 34
  In 32
  Out 32
Enable/Disable Redundant Addresses 12
Encapsulation
  Type 34
Environment_Filter 85
EnvMon Application 76
  Power Supply Status 77
  Temperature Status 77
  Voltage Status 77
Ethernet 153
Ethernet Application 80
event messages 14

F

Fast 123
FDDI 153
Flash
  Memory 62
  Size 62
Flash Application 61
Flash Configuration View 62
Flash Copy Operations Table View 63
Flash Device Chip Properties Table View 62
Flash Device Partition Properties Table View 66
Flash Device Properties Table View 65
Flash File Properties Table View 65
Flash Miscellaneous Operations Table View 66
Flash Partitioning Operations Table View 67
Flow Control 81
Format Error 34
Forward 33
Forwarded 34

G

Group
  IPM Route 93
Group Address 91, 93, 97
  IPM Route 87

H

Hardware
  Revision Level 41
  Ver. 40
Hardware_Configuration_Filter 85
Hellotime 152
Hold Time 102
Hot Standby Router Protocol (HSRP) 149
HSRP Group 150, 153, 154

I

Icons
  Interface, Device View 18
ICP
  In 33
  Out 33
Idle Time out 82
IF Index 90, 150, 153, 154, 155
IGMP 96
Interface 122, 124
  Detail view 20
  Type, Device 18
Interface Configuration 20
Interface Icon Subviews Menu 20
IP
  Accounting Table 29
IP Multicast Routing 87
  Diff In IF Packets 88
  Enable 88
  Group Address 87
  Octets 88
IP multicasting 87, 95
IPC
  Count 34
  Error Count 34

IPM Route Boundary Table 90
Address 91
Address Mask 91
IF Index 90
Status 91
IPM Route Enable, Button 88
IPM Route Interface Table 90
IF Index 90
In Mcast Octets 90
Out Mcast Octets 90
Protocol 90
Rate Limit 90
TTL Threshold 90
IPM Route Next Hop Table 88
Address 89
Closest Member Hops 89
Expiry Time 89
Group 88
IF Index 89
Packets 89
Protocol 89
Source 88
Source Mask 89
State 89
Up Time 89
IPM Route Table 87
Diff In IF Packets 88
Expiry Time 88
Group 87
IF Index 87
IPM Route Enable 88
Octets 88
Packets 88
Protocol 88
Source 87
Source Mask 87
Up Time 88
Upstream Neighbor 87

J

Join/Prune 96
Invalid Messages 102

L

LANCE Ethernet 153
Launching CiscoView 11
Learned Hello Time 152
Learned Hold Time 152
Local Destination 34
Location 81

M

MAC
In 32
Out 32
Metric Out 33
Model
Information 169
Model Information 20
Modem Control 81
Modem Line Configuration Table
View 57
Modem Line Speed Statistics Table
View 60
Modem Line Statistics Table
View 59
Modem Line Status Table View 53
Modem States 53
Monitor Performance 12

N

NBMA interfaces 89, 94
Network
Traffic
Flow 29
Type 19
No Charge 33
Node 111, 126
Non-volatile RAM
Size (bytes) 51
Used (bytes) 51
Not
Forward 33
LAN 33
Novell
Accounting Table 31
Check Point Accounting Table 31
Check Point Information 30

IPX Accounting Information 30
Service Advertisement Protocol View 30
Novell Internet Packet Exchange View 30
Novell Routing Application 30
Number
of Chassis Slots 51

O

Octets 88
In Mcast 90
Out Mcast 90

P

Packets 29, 89
Performance View 156
Physical Index 158
PIM 95
Cisco 102
Component Hold Time 102
Component Table 101
IPM Route Table 97
MIB (RFC 2934) 102
Rendezvous Point Sets 98
PIM Component Table 101
BSR Address 102
BSR Expiry Time 102
Hold Time 102
Index 101
Status 102
PIM Interface
Configuration 96
Designated Router 96
Table Entry View 96
PIM Interface Table 96
Address 96
CBSR Preference 97
Hello Interval 96
IF Index 96
Join Prune Interval 96
Mode 96
Net Mask 96
Status 96
PIM InterfaceTable
Designated Router (DR) 96
PIM IPM Route Next Hop Table 99
Address 100
Group Address 99
IF Index 100
Prune Reason 100
Source Address 99
Source Mask 99
PIM IPM Route Table 97
Assert Metric 98
Assert Metric Preference 98
Group Address 97
Route Flags 98
RPT Bit 98
Source Address 97
Source Mask 98
Upstream Assert Time 98
PIM Neighbor Table 97
Expiry Time 97
IF Index 97
IP Address 97
Mode 97
Up Time 97
PIM-SM Domain 101
Ping Application 68
Ping Request Table View 68
Pix_Firewall_Filter 85
Port Number, Device 18
Port Route Settings 12
Power Supply Status 77
Preempt 151
Preempt Delay 151
Preferred Addresses 160
Priority 150, 154
Protocol 88, 89
Tunnel 104
Protocol Independent Multicasting (PIM) 95
Protocol_Filter 84
Proxy Count 34
Pruned 89, 91
Purpose 7

Q

Queue Application 71

Queue Interface View 71
Queue Rotation Interface View 72
Queue Statistics View 71
QUICC Ethernet 153

R

RAM Information 51
Received, Vines Broadcast 33
Reconfigure Model 161
Redundancy and Model Reconfiguration Options 160
Rendezvous Point Sets 98
Rendezvous Point Sets Table 98
  Address 99
  Component 98
  Expiry Time 99
  Group Address 98
  Group Mask 99
  Hold Time 99
Replies
  Rec 35
  Sent 35
Request
  Out 35
  Rec 35
Required Reading 7
RFC 2024 121, 122
RFC 2281 153
ROM
  Information 51
  Monitor Version 51
  Software Version 51
Row Status 153, 154, 155
RPF neighbor 98
Running Configuration Changes 165

S

Secondary Address 154
Secondary Address Panel 20
Security_Filter 85
Serial Number 40
Session
  Table 82
  View 82
Set Environment Variables 11
Slot 40
SMT
  Table 78
SMT Table View 78
Software
  Version 40
Software_Filter 85
Source 29
Source Address 87, 91, 93, 97
Source Mask 87, 89, 91, 93, 98
SPECTRUM Model 9
SPECTRUM Views documentation 20
Speed
  In 81
  Out 81
Standby Router 152
State, IPM Route Next Hop 89
Status 81
STUN
  Groups View 38
  Ports View 38
  Routes View 39
Sub-Interfaces 20
Supported Devices 8
System
  CPU RAM (bytes) 51
System_Filter 84

T

Task
  Configure the Device 12
  Create Messages 12
  Creating LANs 12
  Enable or Disable Redundant Addresses 12
  Launch CiscoView 11
  Monitor Performance 12
  Port Route Settings 12
  Set Connections 11
  Set Environment Variables 11
  Set Thresholds 12
  Update the Ping Request List 12

Index

View Current Interface/Port Status 13
View IF/Port/App Statistics 13
View/Change Interface IP Address 13
TCP Configuration 137
Temperature Status 77
Term Type 81
Terminal Server
Line View 81
Session View 82
Terminal Server Application 80
Line Configuration View 80
Terminal Server Line View 81
Terminal Server Session View 82
Thresholds 20
Time to Live 90
Token Ring 153
Tracked IF 153
Transmitted 33
Transport Connection Config View 116
Transport Connection Operation Config View 119
Transport Connections 116, 119
Configuration 116
Direct Configuration 121
Operation 119
Specific 121, 122, 123, 124
Trap Configuration 20
Trap Control 125
TS Session Table 82
TTL 89, 90
Type 40, 81

U

Unicasts 34
Update Ping Request List 12
Upstream Neighbor 87
Use Burned In Address 155
Use Configured Timers 151

V

VCL Table 72
VGANYLAN 153
View Current Interface/Port Status 13
View IF/Port/App Statistics 13
View/Change Interface IP Address 13
Vines
Broadcast
Detail View 33
Packets 33
Statistics 33
Echo
Packets 32
Statistics 32
ICP 32
Metric Notification 33
Packets 33
Statistics 33
Interprocess Communications Protocol 32
Routing
Echo View 32
ICP View 32
Rx View 34
Tx View 34
Vines Routing Application 32
Virtual IP Address 152
Virtual MAC Address 153
Voltage Status 77

X

XNS
Echo
Reply 35
Echo Statistics 35
Routing
Application Views 35

Index